

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C.**

In the Matter of	)	GN Docket No. 20-111;
	)	ITC-214-20090105-00006;
<b>Pacific Networks Corp. and</b>	)	ITC-214-20090424-00199
<b>ComNet (USA) LLC</b>	)	

To: The Commission

**RESPONSE TO ORDER INSTITUTING PROCEEDING ON REVOCATION AND  
TERMINATION**

**PACIFIC NETWORKS CORP.  
COMNET (USA) LLC**

Jeff Carlisle  
Stephen Coran  
Rebecca Jacobs Goldman

*of*

Lerman Senter PLLC  
2001 L Street, NW, Suite 400  
Washington, D.C. 20036  
(202) 416-6768  
*Their Counsel*

April 28, 2021

## SUMMARY

On March 17, 2021, the Commission adopted an Order Instituting Proceeding on Revocation and Termination (“*Order*”) establishing a written process for determining whether the Commission should revoke and/or terminate the section 214 authorizations held by Pacific Networks Corp. (“Pacific Networks”) and ComNet (USA) LLC (“ComNet,” and, together with Pacific Networks, the “Companies”) and reclaim ComNet’s International Signaling Point Codes (“ISPCs”). Notwithstanding the hundreds of pages of materials provided in response to an Order to Show Cause (“*OSC*”) issued by the International, Wireline Competition and Enforcement Bureaus last year, the *Order* states in its first paragraph that the Commission took this step because the Companies “have failed at this stage to dispel serious concerns regarding their retention of section 214 authority in the United States,” concerns the *Order* states are based on the Companies’ “ties to the Chinese government” and the asserted coercive effect of Chinese laws allegedly compelling cooperation with espionage.

The *Order* thus immediately lays bare the fundamental substantive and procedural flaw of this entire proceeding as it has been conducted so far: the Commission has not demonstrated that the Companies have ever carried out any nefarious activities at the bidding of the Chinese government, has based its case entirely on speculation that the Companies will act according to foreign influence, and has castigated the Companies for failing to prove the negative that they are *not* subject to foreign influence. As the Companies stated in their response to the *OSC* (the “OSC Response”), neither Company has been asked by the Chinese government or the Chinese Communist Party to take any action that would “jeopardize the national security and law enforcement interests of the United States” or suggest that the Companies are vulnerable “to the exploitation, influence, and control of the Chinese government.” But the *Order* expounds at

length on the theoretical possibility that the Companies’ networks might be used to take such action, ignoring or waving away questions about whether Chinese law is as coercive as the *Order* asserts or concerns about the very real negative consequences to U.S. employees and consumers. The security offered by revocation is wholly performative: it is a solution that the *Order* fails to show will address a real threat or improve the security of U.S. telecommunications networks.

Moreover, the *Order* attempts to bolster its case by developing a theory that the Companies told Team Telecom one thing, then told a Senate subcommittee another thing, then told the Commission yet another thing. As a result, the *Order* repeatedly impugns the truthfulness and transparency of the Companies. But the Companies’ alleged “discrepancies” are nothing of the sort—as the Companies explain herein, representations to the Senate subcommittee regarding the location of databases were not accurately recounted in the subsequent report of the investigation, and representations to the Senate subcommittee regarding ComNet’s operations were consistent with what was stated in the OSC Response.

In the end, the *Order* does not change the underlying objective of the *OSC*: the Commission wants to revoke the Companies’ authorizations for the sole reason that an investment company owned by the People’s Republic of China holds an indirect ownership interest in the Companies in excess of 50%, not because the Commission is aware of any intervention in the Companies by the Chinese government or particular vulnerabilities in the Companies’ services, operations or networks. The *Order* does, however, show even more clearly that the Commission is ignoring or rewriting numerous longstanding protections for holders of authorizations in order to prosecute this case. The Commission shifted the burden of proof, chose a less stringent standard of proof for itself than the law requires, refused to acknowledge that material facts are in dispute when they clearly are in dispute, expanded the

grounds justifying revocation to the point where there is now no reasonable constraint on the Commission's revocation powers, refused to hold a hearing, refused to provide the expert agencies sufficient time for input, proceeded without a recommendation from those expert agencies, refused to review any of the procedural or substantive questions raised by this extraordinary and novel process in a rulemaking proceeding, and refused to conduct any analysis as to whether the risks it has identified could be mitigated. While any one of these procedural shortcuts would raise serious concerns about the Commission's process, together they amount to a proceeding that is arbitrary, capricious and an abuse of discretion, and a denial of the Companies' due process rights.

Pacific Networks and ComNet provide responses to the Commission's further questions on its structure and operations below, and further explain that the Companies' independent operations are not subject to exploitation, influence, or control of the Chinese government, nor has there been any showing that they are or have acted as such.

On review of the information provided herein, the Commission should decline to revoke or terminate the Companies' Section 214 authorizations or reclaim ComNet's ISPCs, and instead consider mitigation measures that will provide a trustworthy and enforceable means for the federal government to monitor the Companies' ongoing compliance. If the Commission is unwilling take those steps, it should order a hearing to provide the Companies an opportunity to dispute the facts on which the Commission intends to rely before a neutral finder of fact.

## TABLE OF CONTENTS

I.	BACKGROUND .....	4
II.	DEMONSTRATION OF WHY REVOCATION AND/OR TERMINATION IS NOT WARRANTED .....	7
A.	No Evidence Tying the Companies to Threats to National Security .....	8
B.	The Coercive Effect of Chinese Laws are not as Clear as the <i>Order</i> Asserts .....	10
C.	The Companies Did Not Provide Inconsistent Information or Intentionally Omit Information from the OSC Response Provided to the U.S. Government .....	13
D.	<i>Pro Forma</i> Notifications Have Never Been Used as a Basis for Revocation .....	16
E.	The Order Improperly Fails to Consider Additional Mitigation Measures .....	17
F.	The <i>Order</i> Fails to Distinguish Among Services.....	22
III.	THE COMMISSION’S PROCEDURE IS FATALY UNFAIR .....	23
A.	The Commission’s Process is Unfair in Light of Precedent .....	24
B.	The <i>Order</i> Improperly Avoids an Evidentiary Hearing.....	29
C.	The <i>Order’s</i> Process Conflicts with the Administrative Procedure Act.....	34
D.	The <i>Order’s</i> Process Conflicts with the Due Process Clause .....	36
E.	The <i>Order’s</i> Assertion that the Commission Can Serve as a Neutral Fact Finder is Unavailing.....	42
IV.	RESPONSES TO QUESTIONS.....	43
V.	SHOULD THE COMMISSION REVOKE THE COMPANIES’ AUTHORIZATIONS, THE COMMISSION MUST PROVIDE A MEANINGFUL TRANSITION PERIOD FOR EXISTING CUSTOMERS .....	83
VI.	CONCLUSION.....	84

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C.**

In the Matter of	)	GN Docket No. 20-111;
	)	ITC-214-20090105-00006;
<b>Pacific Networks Corp. and</b>	)	ITC-214-20090424-00199
<b>ComNet (USA) LLC</b>	)	

To: The Commission

**RESPONSE TO ORDER INSTITUTING PROCEEDING ON REVOCATION AND  
TERMINATION**

Pacific Networks Corp. (“Pacific Networks”) and ComNet (USA) LLC (“ComNet,” and, together with Pacific Networks, the “Companies”), provide this response to the Order Instituting Proceeding on Revocation and Termination (“*Order*”) released by the Commission on March 19, 2021.<sup>1</sup> The Commission directed the Companies to file this response to respond to 31 questions presented in an Appendix to the *Order* and to “demonstrate why the Commission should not revoke and/or terminate their section 214 authority . . . .”<sup>2</sup>

---

<sup>1</sup> *Pacific Networks Corp. and ComNet (USA) LLC*, Order Instituting Proceeding on Revocation and Termination, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199, FCC 21-38 (rel. Mar. 19, 2021). The Companies requested an extension of time until May 12, 2021 to file this response, and neither a grant nor a denial had issued as of the time of filing. The Companies have elected to file on the original due date. Given their need for additional time, however, they will file supplemental information if necessary and request that Commission staff contact them if they believe additional information is necessary beyond what could be provided within the timeframe allowed.

<sup>2</sup> See *Order* at ¶ 75. For ease of reference, the Companies will use the term “revoke” to refer to “revoke and/or terminate.”

Since the Order to Show Cause (the “OSC”) issued in this docket, the Companies’ §documents,<sup>3</sup> the Executive Branch agencies provided input (though no recommendation),<sup>4</sup> and the Commission issued the *Order*. Yet, the Commission and the Companies find themselves in very much the same position in which they started over a year ago: there has not been a single allegation of any misrouting, hijacking of traffic or other bad behavior indicating the Companies have used their services to facilitate any national security threat from China or that they have any intent to do so. The *Order* directed the Companies to demonstrate why the Commission should not revoke their section 214 authorizations, and the Companies do so, again, as detailed below. The *Order* also directed the Companies to answer more detailed questions about their operations and governance and the Companies do so, again, as detailed below. But the *Order* also reiterated the same inferences and assumptions that formed the basis of the *OSC* and of similar recent revocation proceedings, most of which are disputed by the Companies. The *Order* went to great lengths to impugn the Companies’ truthfulness and transparency when a simple conversation with the Company would likely have resolved most of the Commission’s apparent concerns.

Thus, while this response addresses the supposed discrepancies and omissions raised in the *Order*, the outcome of the process directed by the *Order* is all but already written. This process turns its back on numerous Commission precedents and protections by, among many other things, rejecting the need for an evidentiary hearing, shifting the burden of proof, and applying a less stringent burden than the Commission is required to meet. The *Order* argues at

---

<sup>3</sup> Response to Order to Show Cause, *Pacific Networks Corp. & ComNet (USA) LLC*, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (filed June 1, 2020).

<sup>4</sup> The Companies intend the term “Executive Branch agencies” to encompass the same agencies encompassed by the term as used in the *Order*. *Order* n.3.

length about the Commission’s discretion to proceed without a hearing, even going so far as to propose that the hearing would provide no benefit and, remarkably, might even cause harm. The *Order* fails to explain, though, how its sheer number of changes to longstanding policies could possibly result in a fair process, especially given the extent of disputed facts in question. As shown below, this revocation proceeding is arbitrary, capricious and an abuse of discretion, and separately amounts to a denial of the Companies’ due process rights.

Notably, the *Order* pays scant attention to the Companies’ repeated offers to discuss mitigation, reiterating the unsubstantiated conclusion that the identified security risks could not possibly be mitigated. The *Order* ignores the fact that the Companies have complied with the Letter of Assurance that has been in place since 2009, and sidesteps the fact that the Executive Branch expressly did not, as it could, recommend revocation. The Companies propose several measures that would directly address the concerns identified by the *Order*. Moreover, while the *Order* cites to the alleged security risks of the multi-protocol label switching virtual private networks (“MPLS VPN”) service provide by Pacific Networks, and may consider ComNet’s Wholesale International Direct Dial (“IDD”) service threatening because of the asserted risks of interconnection, the *Order* provides no explanation of what national security risks might be presented by ComNet’s Retail Calling Card service—a prepaid service used by hundreds of thousands of customers for the sole purpose of reaching international numbers. It would thus appear that there are a number of options for the Commission and the Companies to explore to see what measures might be taken short of simply stripping the Companies’ authorizations altogether.

But should the Commission elect to move forward to revoke the Companies’ authorizations and reclaim ComNet’s ISPCs, and as stated in the OSC Response, the Companies



in no way waive or otherwise wish to forego an evidentiary hearing before an Administrative Law Judge at which the Commission would bear the burden of proof before a neutral arbitrator under a clear and convincing evidentiary standard.

## **I. BACKGROUND**

The Companies hereby incorporate by reference the background facts provided in the OSC Response.

Notwithstanding the Companies' openness to exploring discussions regarding mitigation, the Companies received no substantive inquiries or requests for clarification from the Commission following the filing of the OSC Response on June 1, 2020. Almost six months after the Companies filed the OSC Response, the International Bureau ("Bureau") provided the Department of Justice ("DoJ") 30 days to provide the views of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (generally known as "Team Telecom") on the Companies' "arguments concerning whether and how they are subject to the exploitation, influence, and control of the Chinese government, and the national security and law enforcement risks associated with such exploitation, influence, and control."<sup>5</sup> The Bureau also asked "whether additional mitigation measures could address any identified concerns." On the same day, the Bureau sent a similar request for input into its concurrent inquiry regarding whether China Unicom's Section 214 authorizations should be revoked.<sup>6</sup>

---

<sup>5</sup> Letter from Denise Coca, Chief, Telecommuns. & Analysis Div., Int'l Bureau, FCC, to Sanchitha Jayaram, Chief, For. Investment Rev. Sec., Nat'l Security Div., Dep't of Justice, GN Docket No. 20-111, FCC File Nos. ITC-214-20090105-00006; ITC-214-20090424-00199, DA 20-1216 (Oct. 15, 2020) ("Bureau Request Letter") at 3.

<sup>6</sup> Letter from Denise Coca, Chief, Telecommuns. & Analysis Div., Int'l Bureau, FCC, to Sanchitha Jayaram, Chief, For. Investment Rev. Sec., Nat'l Security Div., Dep't of Justice, GN

On November 16, 2020, the Executive Branch agencies filed a 13-page response to the Commission, being careful in the first paragraph to state that “[g]iven the nature of the Commission’s request for views on discreet factual questions, and the limited time allotted for response, this response is not offered as a recommendation by the Committee . . . that the FCC take any particular action with respect to the Companies.”<sup>7</sup> The response is notable for three other reasons.

First, nowhere does the response actually address any of the Companies’ arguments, as requested by the Bureau. Rather, the letter reiterates arguments raised against China Telecom and China Unicom regarding the “inherent national security risks attach[ed] to telecommunications companies owned or controlled by the Chinese government” and the asserted coercive effect of Chinese law.<sup>8</sup> The letter concludes that no mitigation measures could address the national security risks, not as a result of an analysis of the Companies’ circumstances or any mitigation measures, but solely because of “[t]he Chinese government’s ultimate ownership over the Companies.”<sup>9</sup>

---

Docket No. 20-110, FCC File Nos. ITC-214-2020728-00361; ITC-214-20020724-00427, DA 20-1215 (Oct. 15, 2020).

<sup>7</sup> Letter from Kathy Smith, Chief Counsel, Nat’l Telecommuns. & Information Admin., to Denise Coca, Chief, Telecommuns. & Analysis Div., Int’l Bureau, FCC, GN Docket No. 20-111 FCC File Nos. ITC-214-20090105-00006; ITC-214-20090424-00199 (filed Nov. 16, 2020) (“Executive Branch Agencies Letter”) at 1.

<sup>8</sup> *Id.* at 2.

<sup>9</sup> *Id.* at 11.

Second, except for a handful of specific references to the Companies and their operations,<sup>10</sup> the analysis provided by the response is general, not specific to the Companies, and could be applied to any Chinese state-owned company. The response does not specifically analyze the Retail Calling Card, Wholesale IDD or MPLS VPN services provided by the Companies, instead simply concluding that the very interconnection of the Companies’ networks provides “an opportunity for exploitation.”<sup>11</sup> The general language of the response is substantially a copy of language provided in the Executive Branch agencies’ separate, much longer, response regarding China Unicom.<sup>12</sup>

Third, the response not only expressly pointed out that it was not a “recommendation,” it also stated that DoJ and Department of Homeland Security (“DHS”) “have not identified acts of non-compliance under the minimal conditions placed on the Companies’ Section 214 authorizations.”<sup>13</sup> Importantly, the Executive Branch Agencies Letter reports this conclusion even though DoJ and DHS have authority under the Letter of Assurance filed with the Commission in 2009 (as a condition to the Companies receiving section 214 authority) to “request that the FCC modify, condition, revoke, cancel, or render null and void any relevant

---

<sup>10</sup> See *id.* at 2 (noting ultimate ownership by CITIC Group Corporation), 6 (again noting ownership by CITIC), 8 (describing the addition of unregulated services to the Companies’ services offered under Section 214), 10 (noting the agencies “have not identified acts of non-compliance”).

<sup>11</sup> *Id.* at 8, 10.

<sup>12</sup> See Letter from Kathy Smith, Chief Counsel, Nat’l Telecommun. & Information Admin., to Denise Coca, Chief, Telecommun. & Analysis Div., Int’l Bureau, FCC, GN Docket No. 20-110, FCC File Nos. ITC-214-2020728-00361; ITC-214-20020724-00427 (filed Nov. 16, 2020).

<sup>13</sup> Executive Branch Agencies Letter at 10.

license, permit, or other authorization granted by the FCC to Pacific Networks, CM Tel, or any successor-in-interest to either.”<sup>14</sup>

## II. DEMONSTRATION OF WHY REVOCATION AND/OR TERMINATION IS NOT WARRANTED

As a foundational matter, the Commission should not revoke the Commission’s authorizations under Section 214 because nothing in the record demonstrates that the Companies have engaged in any conduct constituting a threat to national security, and the Commission has not expressed a rationale for revocation by clear and convincing evidence that allows a departure from the Commission’s precedent. The Commission’s entire case rests on a faulty premise: that state-owned Chinese actors, of all the foreign-owned entities that hold Section 214 authorizations, are so particularly given to engaging in threats to U.S. national security that they warrant being singled out not only for revocation, but for a process that is demonstrably inquisitorial, prejudicial and unfair. The *Order* attempts to bolster this case by adding and repeating alleged discrepancies between the OSC Response and report of the Permanent Senate Subcommittee on Investigations (the “PSI Report”),<sup>15</sup> and by charging that the Companies provided material information to the Senate Subcommittee and Team Telecom but omitted that information in their response to the *OSC*. The Companies have not, however, provided

---

<sup>14</sup> Letter from Norman Yuen, Pacific Networks, and Fan Wei, CM Tel, to Stephen Heifetz, DHS and Matthew G. Olsen, DOJ, File Nos. ITC-T/C-20080913-00428, ITC-214-20090105-00006 (Mar. 3, 2009) (“2009 Letter of Assurance”) at 4.

<sup>15</sup> Staff Report of Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, 116th Congress, Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers (June 9, 2020), *available at* <https://www.hsgac.senate.gov/download/threats-to-us-networks-oversight-of-chinese-government-owned-carriers>.

inconsistent information, nor did they intentionally withhold information provided to other arms of the U.S. government.

**A. No Evidence Tying the Companies to Threats to National Security**

As the Companies pointed out in the OSC Response in 2020, and as continues to be true a year later, the Companies have never been asked by the Chinese government to take any actions detrimental to U.S. security, and there has been no evidence that the Companies have engaged in any actions that would constitute a threat to national security. There have been no allegations of misrouting, no allegations of hijacking U.S. government communications, nothing. Despite ongoing monitoring under the 2009 Letter of Assurance, which included a number of exchanges of substantial information as explained in the OSC Response and a specific inquiry by the Commission to the Executive Branch agencies, the Commission does not identify any non-compliance with the Companies' national security-related obligations.

One might reasonably respond that the Commission need not wait until after a potentially disastrous violation of national security has occurred to take action. But that would presume there was a rational basis for believing that these Companies, in particular, are likely to engage in behavior that would lead to such a violation. The *Order* certainly does not provide any reason specific to the Companies. A review of the asserted threats shows that all of them stem from nothing more than interconnection to the telecommunications network by U.S. companies that are partially state-owned, not that there is anything in particular about the Companies' services or operations that increases that risk.

It is particularly telling that the *Order* scarcely performs any specific analysis of the Companies' services provided under Section 214, and the analysis it does perform is actually wrong. The *Order* includes no analysis of any national security threats posed by ComNet's

Wholesale IDD and Retail Calling Card services, instead only speculating about possible misuse of personally identifiable information (“PII”) and customer proprietary network information (“CPNI”) ComNet may hold as a result of providing such services.<sup>16</sup> As shown in response to Questions 9 and 12, below, ComNet’s handling of any such information is subject to policies that are typical of those adopted by other telecommunications carriers. The protection of CPNI is, in any event, particularly within the jurisdiction of the Commission. As regards Pacific Networks’ MPLS VPN service, the *Order* does assert that “Pacific Networks’ MPLS VPN service involves the use of Points of Presence to peer with other providers using Border Gateway Protocol (BGP) routers,” and then notes that “the offering of IP Transit services in the form of using BGP is a prime candidate for security exploitation.”<sup>17</sup> As explained in response to Question 16, however, Pacific Networks does not provide IP Transit services as described in the *Order*. Thus, the one assertion so far in the record specific to any service provided by the Companies is incorrect. Given the paucity of any actual analysis showing a national security threat, it is unsurprising that the *Order*, over a year into this proceeding, should now seek further information on ComNet’s Voice over Internet protocol “VoIP” service, which is not even subject to regulation under Section 214.<sup>18</sup> It is difficult to escape the conclusion that this proceeding is an exercise in

---

<sup>16</sup> *Order* at ¶ 51.

<sup>17</sup> *Id.* at ¶ 45 & n.219.

<sup>18</sup> *Id.* at ¶ 48 & n.231. The *Order* directed the Companies “to fully explain the IP service offering or whether this is an interconnected VoIP service offering as defined by the Commission’s rules and any security measures concerning this service. See Appx. A.” The *Order* did not include a question on the IP service, so this answer is provided as the answer to Question 32, below.

performative security, rather than an assessment of the risk and magnitude presented by the actual services the Companies provide.<sup>19</sup>

Moreover, the nature of the assertions of national security threats are not in any way unique to the Companies. The *Order* and the Executive Branch Agencies Letter repeatedly describe national security threats that arise solely because of the interconnected nature of networks. There is not a single national security threat identified on the record that the Companies could cause that could not be caused by every other telecommunications and information service provider. The *Order* may explain at length why the government of China presents a security threat to the U.S., and assert that China’s laws can compel U.S. subsidiaries to violate U.S. law, but it does nothing to then explain why non-state-owned Chinese companies do not also present a security threat; why state-owned companies from countries other than China do not present comparable risks; or why non-state-owned companies from countries other than China do not present comparable risks.<sup>20</sup>

Observing the procession of claims against the Companies from the *OSC* to the Executive Branch Agencies Letter to the *Order*, it is clear that there is only one claim: they are (not even wholly) state-owned companies from China.

## **B. The Coercive Effect of Chinese Laws are not as Clear as the *Order* Asserts**

The *Order* concludes that Chinese cybersecurity laws “raise significant concerns” that the Companies will be “forced to comply with Chinese government requests” and demonstrate

---

<sup>19</sup> See *China Mobile International (USA) Inc.*, Memorandum Opinion & Order, 34 FCC Rcd 3361 (2019), Statement of Commissioner Jessica Rosenworcel (“Please don’t get confused by the performative security associated with this decision.”).

<sup>20</sup> See also OSC Response at 27-28 (asking why these questions have not yet been examined in a rulemaking).

control of the Chinese government over the Companies.<sup>21</sup> The *Order* identifies three particular laws that it believes raise these concerns—the 2017 National Intelligence Law, the 2017 Cybersecurity Law, and the 2019 Cryptography Law—without pointing to any evidence that the Companies are, in fact, bound by such laws.<sup>22</sup> Rather, the *Order* points to the PSI Report citing these same conclusions stemming from the possibility of the laws being interpreted in this manner.<sup>23</sup> The PSI Report bases this conclusion on statements by commentators who argue what the laws “could” do if broadly interpreted, yet the plain language of the laws contradicts such interpretation, raising a material question as to the extent of compulsion under the laws as applied to the Companies’ operations.

The National Intelligence Law specifies that its restrictions “shall be conducted in accordance with law . . . and shall *preserve the lawful rights and interests of individuals and organizations*.”<sup>24</sup> As U.S. companies, the Companies are not permitted under U.S. law to support another country’s intelligence gathering activities, thus the National Intelligence Law could not be used to direct such efforts, as it would be in contradiction of the law itself.

The 2019 Cryptography Law referenced in the Order states that cooperation between foreign and Chinese entities regarding commercial encryption will be voluntary and Article 31 of the law bars the State Cryptography Administration and related agencies from demanding source

---

<sup>21</sup> *Order* at ¶ 24.

<sup>22</sup> *Id.*

<sup>23</sup> *See* PSI Report at 28-30.

<sup>24</sup> 2017 National Intelligence Law, Article 8, unofficial translation at <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/> (last accessed April 20, 2021) (emphasis added).



codes and other proprietary information related to cryptography.<sup>25</sup> Accordingly, the Commission cannot conclude that the law would taint the Companies to the extent asserted in the *Order*.

Finally, the *Order* 2017 Cybersecurity Law states that it is “applicable to the construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People’s Republic of China.”<sup>26</sup> The Companies’ network operations in the U.S. would not be subject to the reach of the 2017 Cybersecurity Law.

In addition, the OSC Response showed that the Companies are not subject to certain provisions of China’s 2018 Company Law that would increase the control of the Chinese government over mergers, dissolutions, and other important decisions by wholly state-owned enterprises.<sup>27</sup> The *Order* rejects this, pointing to the Chinese government’s Ministry of Finance holding a 100% stake in CITIC Group Corporation.<sup>28</sup> As the OSC Response pointed out, though, and which the *Order* sidesteps, both CITIC Limited and CITIC Telecom International Holdings Limited (“CITIC Tel”) have substantial percentages of public ownership, and thus neither of the Companies are wholly state-owned. Still, the *Order* tries to ignore the actual application of the 2018 Company Law by pointing to the allegedly coercive effect of the laws discussed above. This is a *non sequitur*: the particular issue at hand is the extent of possible control by the

---

<sup>25</sup> 2019 Cryptography Law, Articles 21 and 31, unofficial translation at <https://www.chinalawtranslate.com/en/cryptography-law/> (last accessed April 21, 2021).

<sup>26</sup> 2017 Cybersecurity Law, Article 2,, unofficial translation by Rogier Creemers, et al., available at <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/> (last accessed April 20, 2021) (emphasis added).

<sup>27</sup> OSC Response at 22-23.

<sup>28</sup> *Order* at ¶ 38.

Chinese government of state-owned enterprises, a crucial assumption of the *Order*. It is telling, however, that the *Order* responds to any possible mitigating fact by falling back on its core, flawed assumptions.

Notably, the *Order* does not cite to any evidence that the Chinese laws have actually been used to compromise the Companies in any way. Rather, the *Order* relies on hypothetical scenarios based on the possibility that the laws could be interpreted in such a way as to impact the U.S.-based entities. The conclusions are not based on fact, or an analysis specific to the Companies' operations. The Companies have repeatedly stated that they have not been asked by the Chinese government to do anything in contradiction of U.S. law and do not believe that they could be asked to do so. The facts, existing outside of hypotheticals, directly contradict the *Order's* conclusions.

In any event, if the federal government were so concerned about the potential impact of these relatively new laws, it had a readily available remedy at its disposal: negotiating amendatory language to the 2009 Letter of Assurance. In effect, the *Order* holds the Companies responsible for the mere adoption of Chinese laws without placing any burden on Team Telecom to meet with the Companies to discuss potential changes to the 2009 Letter of Assurance that would alleviate specific concerns relative to the Companies' services and obligations under the Section 214 authorizations. That opportunity still exists as an alternative to revocation.

**C. The Companies Did Not Provide Inconsistent Information or Intentionally Omit Information from the OSC Response Provided to the U.S. Government**

The *Order* compensates for the lack of actual evidence of bad acts by alleging “discrepancies and omissions” between information the Companies provided to the Senate

Subcommittee and information the Companies provided in the OSC Response. As explained in detail in response to Question 19, the alleged discrepancies are not discrepancies.

An alleged discrepancy regarding the location of databases is actually the result of the PSI Report making a general statement that applied only to databases ComNet uses for its VoIP service, which are located only in the United States. And in any event, the 2009 Letter of Assurance anticipates that U.S. records may very well be stored outside the U.S., and so there is no reasonable argument that storing such data outside the U.S. violates the Companies' obligations. Alleged discrepancies about the Company's day-to-day management, when examined, are not actually discrepancies because they do not show any more involvement by indirect owners into the Companies' day-to-day operations in the U.S. than has been known to Team Telecom since 2009, and anticipated by the 2009 Letter of Assurance on file with the Commission. The 2009 Letter of Assurance specifically states that the Companies would provide Team Telecom descriptions of "system interrelationships between [ComNet's] California switching facility with the Hong Kong network operations center and International Finance Data Center."<sup>29</sup> The Companies did so in 2009, and also provided a Pacific Networks Corp. IT Security Policy, which was derived from the then current version of the CITIC Tel policy, and later succeeded by the CITIC Tel Policy provided to Team Telecom in 2017.<sup>30</sup> The Companies have never insisted that they were utterly cut off from any interaction with CITIC Tel, and the U.S. government has long been aware of the nature of CITIC Tel's guidance to the Companies regarding information security policy.

---

<sup>29</sup> 2009 Letter of Assurance at 2.

<sup>30</sup> See *infra* Section IV, Question 19.

The *Order* asserts that, aside from alleged discrepancies with the PSI Report, the Companies also omitted information they should have provided to the Commission. As explained in response to Question 19, in fact the Companies did provide the Commission with the CITIC Tel policy that appears to be the major basis for this assertion. The Companies provided this information voluntarily, and provided it notwithstanding the fact that—amidst the numerous other very specific questions regarding the Companies’ governance and operations—the *OSC* did not specifically ask for such information. In the end, the *Order* excoriates the Companies for missing an opportunity to provide additional detail that would not have significantly changed the import of the statements in the OSC Response given the exhaustive information the Commission and the Executive Branch agencies already possessed. This does not, however, amount to intentional wrongdoing or any attempt to mislead the Commission.

While it would be reasonable for Commission staff to ask for clarification if there is a misunderstanding regarding information on the record, the *Order* jumps to the conclusion that every possible connection between the Companies and CITIC Tel and every alleged omission is, necessarily, evidence of an intentional and knowing misrepresentation or omission, calling into question the Companies’ transparency and trustworthiness. This is, on its face, unfair, particularly given the amount of information and disclosure the Company has voluntarily provided to the Senate Subcommittee, Team Telecom and the Commission, including the hundreds of pages of documents filed in response to the *OSC*.

**D. *Pro Forma* Notifications Have Never Been Used as a Basis for Revocation**

The *Order* also impugns the Companies’ trustworthiness for their failure to provide a notification of the 2014 *pro forma* transfer of control fully discussed in the OSC Response.<sup>31</sup> As explained in the OSC Response, the Commission has never revoked a Section 214 authorization for failure to make a required *pro forma* notification.<sup>32</sup> The *Order* does not assert that this failure standing on its own would warrant revocation, but rather adds this to the list of “concerns” about whether the U.S. government can “trust [the Companies] to comply with U.S. law and regulations.”<sup>33</sup>

This gratuitous criticism is completely misplaced. Of course, the Companies acknowledge that they should have filed the notification. But the record shows they had no intention whatsoever of hiding the transaction from the U.S. government since the Companies advised Team Telecom about it. There is also no apparent reason for the Companies to have intentionally withheld the information from the Commission. It was a mistake of the same kind the Commission sees every day from Section 214 authorizations holders and licensees of every size and description. If the Commission were to apply this standard to every license and authorization holder for every inadvertent compliance failure, it would very quickly run out of trustworthy regulatees. Moreover, the *Order’s* comment about the Companies’ “continued failure” to file the notification<sup>34</sup> is unnecessarily sharp, as the Companies stated they were

---

<sup>31</sup> OSC Response at 6-7, 33-36.

<sup>32</sup> *Id.* at 34-36.

<sup>33</sup> *Order* at ¶ 60.

<sup>34</sup> *Id.*

prepared to file the notifications on a *nunc pro tunc* basis, but would have appreciated further discussion with Commission staff on the best way to proceed. Given the approach taken in the *Order* on this matter, the Companies will, of course, file the notification after providing this response.

**E. The Order Improperly Fails to Consider Additional Mitigation Measures**

In the 2009 Letter of Assurance, the Companies agreed:

- “to take all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in this letter;”
- “that they will not, directly or indirectly, disclose or permit disclosure of or access to U.S. Records, Domestic Communications . . . to any person if the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. government without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of DHS and DOJ or the authorization of a court of competent jurisdiction in the United States;” and
- “to notify DHS and DOJ . . . of any material changes in any of the facts as represented in [the 2009 LOA], or in notices or descriptions submitted pursuant to this letter” and “of any material changes to their ownership structure.”

In reliance on these agreements, on March 30, 2009, Team Telecom advised the Commission that it had no objection to grant of the Companies’ Section 214 applications, conditioned on the Companies’ adherence to 2009 Letter of Assurance.<sup>35</sup>

Tellingly, neither the *Order* nor the Executive Branch Agencies Letter found any violations of the 2009 Letter of Assurance, and the *Order* states only that the “record evidence warrants a closer examination of the [2009 Letter of Assurance] given the apparent inconsistent statements made by Pacific Networks and ComNet to the Senate Subcommittee, the Executive

---

<sup>35</sup> DoJ and DHS Petition to Adopt Conditions to Authorizations and Licenses, File Nos. ITC-T/C-20080913-00428, ITC-214-20090105-00006 (filed Mar. 30, 2009).

Branch agencies, and the Commission.”<sup>36</sup> Nevertheless, the *Order* concludes that the Commission is “not persuaded by Pacific Networks’ and ComNet’s argument that mitigation measures could address specific concerns about any security vulnerabilities.”<sup>37</sup> Its basis for this conclusion is the Executive Branch Agencies Letter.

As explained above, DoJ and DHS have authority under the 2009 Letter of Assurance to “request that the FCC modify, condition, revoke, cancel, or render null and void any relevant license, permit, or other authorization granted by the FCC to Pacific Networks, CM Tel, or any successor-in-interest to either.”<sup>38</sup> But the Executive Branch Agencies Letter states that “the Monitoring Agencies have not identified acts of non-compliance under the minimal conditions placed on the Companies’ Section 214 authorizations”<sup>39</sup> and the letter decidedly “is not offered as a recommendation . . . that the FCC take any particular action with respect to the Companies.”<sup>40</sup>

It appears, however, that the *Order*, the Executive Branch agencies, and the Senate Subcommittee are now discounting those earlier protections, apparently as a way of discounting any possible ameliorative effect of mitigation. The Executive Branch Letter states that “[m]uch like the national security environment, the Companies are not the same providers today that they

---

<sup>36</sup> *Order* at ¶ 63.

<sup>37</sup> *Id.* at ¶ 67.

<sup>38</sup> 2009 Letter of Assurance at 4.

<sup>39</sup> Executive Branch Agencies Letter at 10.

<sup>40</sup> *Id.* at 1.

were when they executed the Letter of Assurance,”<sup>41</sup> pointing to the different services the Companies now offer. The Senate Subcommittee, on the other hand, focused on oversight by Team Telecom, finding that “[e]ven where a security agreement was entered, Team Telecom’s process for monitoring compliance with that agreement was haphazard.”<sup>42</sup> The PSI Report proceeds to detail systemic failures of the oversight process:

**Team Telecom was an informal group, with no statutory authority. As a result, its review of foreign carriers’ applications was ad hoc, leading to delays and uncertainty.** Throughout its existence, Team Telecom operated under no formal legislative or regulatory authority. Instead, it reviewed foreign carriers’ applications at the request of and under the powers of the FCC. The lack of statutory authority resulted in a disorganized, haphazard, and lengthy review process that has been heavily criticized and referred to as an “inextricable black hole.” Team Telecom had no deadlines by which it needed to make recommendations to the FCC, meaning the review of an application could—and often did—last years.

**The lack of statutory authority also prohibited Team Telecom from conducting meaningful oversight of foreign carriers authorized by the FCC.** Team Telecom’s monitoring and oversight capabilities existed only when it signed a security agreement with a foreign carrier. But, it was limited to monitoring compliance with the particular terms of the agreement. The stringency of these agreements increased over time, but historical agreements—particularly those entered before 2010—were written broadly, such that Team Telecom had little to verify. Further, Team Telecom did not start to develop an interagency process for monitoring compliance with security agreements until 2010 or 2011.<sup>43</sup>

The OSC Response contradicts parts of this analysis, instead showing that the communications between Team Telecom and the Companies were regular, provided extensive information on the Companies’ operations, and were characterized by DoJ as “comprehensive

---

<sup>41</sup> *Id.* at 8.

<sup>42</sup> PSI Report at 39.

<sup>43</sup> *Id.* at 9-10.



and informative.”<sup>44</sup> But it is notable that, in its zeal to evict the Companies, the *Order* ignores the systemic problems identified in the PSI Report and ignores the Executive Branch Agencies Letter’s refusal to make any specific recommendation or even find a violation of the 2009 Letter of Assurance.

The *Order* ignores these important points because it wants to avoid substantively addressing the question of mitigation. The *Order* acknowledges that “‘framed by the Commission’s articulation of current national security concerns, *those* mitigation conditions would not address the current law enforcement and national security risks identified both by Congress and the Commission.’”<sup>45</sup> If “those” mitigation measures from 2009 are inadequate in 2021, then the appropriate approach is for the Commission and Team Telecom to consider what mitigation measures will be successful in the changed national security environment. Just as Team Telecom signed off on the 2009 Letter of Assurance to address national security concerns that existed at that time, so too could Team Telecom have at least attempted to the same to address the change national security environment stemming from adoption of Chinese law in the intervening years.

The linchpin for the Commission’s determination that mitigation measures cannot resolve national security concerns appears to rest on a single statement in the Executive Branch Agencies Letter stating that “[p]ut simply, mitigation requires a minimum level of trust, and that level of trust is absent here.”<sup>46</sup> But here, the Executive Branch Agencies Letter provides no analysis or

---

<sup>44</sup> OSC Response at 7-9.

<sup>45</sup> *Order* at ¶ 93, *quoting* Executive Branch Agencies Letter at 2 (emphasis added).

<sup>46</sup> Executive Branch Agencies Letter at 11.

findings supporting their conclusion that they cannot trust the Companies, which have consistently complied with their obligations under the 2009 Letter of Assurance. The Commission is relying on unsupported *dicta* that is contradicted by the Companies’ record of cooperation with Team Telecom, and which appears in a letter that provides no specific recommendations and conducts no analysis specific to the Companies.

As for the Commission’s concerns about the Companies’ “ability to cooperate and be fully transparent with the Executive Branch agencies,”<sup>47</sup> the Companies reiterate that they have complied with the 2009 Letter of Assurance, were “comprehensive and informative” in their dealings with Team Telecom, and that Team Telecom did not, as it clearly could have, “request that the FCC modify, condition, revoke, cancel, or render null and void any relevant license, permit, or other authorization granted by the FCC to Pacific Networks, CM Tel, or any successor-in-interest to either.”<sup>48</sup> Rather than considering the Companies’ compliance with the 2009 Letter of Assurance over the past 12 years, the Commission ignores the Companies’ cooperation with Team Telecom and instead relies solely on alleged inconsistencies in statements made to the Senate Subcommittee and the Commission in response to the *OSC*, fully discussed above and in response to Question 19.

What appears clear is that there are a number of questions about whether mitigation measures can be effective, which the *Order* did not even raise, much less analyze. The PSI Report described the systemic problems with Team Telecom’s oversight of the 2009 Letter of Assurance, so it cannot be simply presumed that mitigation measures will be unsuccessful when

---

<sup>47</sup> *Order* at ¶ 69.

<sup>48</sup> *Id.* at ¶ 62.

the PSI Report itself concluded that the government failed in its oversight of the mitigation measures that did apply. It is at best premature for the Commission to state that mitigation measures will not work when it has not even given any reasoned consideration to specific conditions. In the OSC Response, the Companies made clear that they “are willing to provide additional ongoing assurances through a binding mitigation agreement to supplement or replace the existing Letter of Assurance.”<sup>49</sup> A non-exhaustive list of additional mitigation measures could include the following:

- storage of all customer records at facilities in the United States, with any redundancy also at facilities in the United States;
- access to customer and network records limited to United States citizens;
- pre-launch review of new services offered in the United States;
- quarterly compliance reporting under penalty of perjury; and
- annual or semi-annual Team Telecom site visits.

Even if a combination of specific mitigation measures did not explicitly address every conceivable risk, the application of a range of compliance measures and regular reporting with Team Telecom would effectively eliminate any value the Companies’ operations might have for any foreign threats to national security.

#### **F. The *Order* Fails to Distinguish Among Services**

As noted above, the *Order* incorrectly assesses the threat posed by Pacific Networks’ MPLS VPN service, and fails to identify any specific national security threats posed by ComNet’s Wholesale IDD and Retail Calling Card services, apart from customer information

---

<sup>49</sup> OSC Response at 25.

already acknowledged to be within the Commission’s regulatory control and subject to its usual enforcement processes. The *Order* does discuss various characteristics of interconnected networks and VoIP service and the threats posed thereby, but fails to link any of these generalized concerns to the services at issue. The *Order* thus fails to show that any one of these services presents such a particularized threat that removing the Companies’ Section 214 authorizations to provide any telecommunications services is warranted.

### III. THE COMMISSION’S PROCEDURE IS FATALY UNFAIR

If, despite the showing above and the responses to the Commission’s questions, the Commission nevertheless believes revocation is warranted, the Commission must order an evidentiary hearing as requested by the Companies in the OSC Response.<sup>50</sup> While the *Order* explains at length why it is within the Commission’s discretion to hold a hearing, a review of the Commission’s precedent on administrative hearings and a host of other procedural protections show that the Commission has taken every possible shortcut in order to pursue a case for revocation against the Companies. That is the opposite approach the Commission should take when the consequences are as severe as they are here—effectively shutting down two companies’ businesses. Taken together, the Commission’s refusal to afford the Companies the procedural protections usually afforded in revocation proceedings, with a minimum of explanation in the *Order*, is arbitrary, capricious and an abuse of discretion, and separately denies the Companies their rights to due process.

---

<sup>50</sup> *Id.* at 36-37.

**A. The Commission’s Process is Unfair in Light of Precedent**

The further process created by the *Order* is an illusion of fair process. As explained in the preceding section, it could not be clearer from the *Order* that the Commission took every opportunity to interpret the evidence in a way most supportive of revoking the Companies’ authorizations, and that the process now is little more than an opportunity for the Commission to plug whatever gaps it may need to plug to strengthen its case for revocation. This so-called additional process does, however, confirm that the Commission has ignored or waved away numerous protections that have long been hallmarks of the Commission’s process. Specifically:

- While the Commission’s precedent makes clear that the Commission and the Bureaus bear the burden of proof when seeking to revoke a license or authorization,<sup>51</sup> the *Order* insists on placing the burden of proof in this proceeding on the Companies by requiring them to prove the negative proposition that they are not subject to exploitation by a foreign state. The *OSC* placed the burden on the Companies to show why a revocation proceeding should not be initiated, and in the very first paragraph of the *Order* the Commission states that the Companies “have failed at this stage to dispel serious concerns regarding their retention of Section 214 authority.”<sup>52</sup> Thus, having started this proceeding with no evidence that the Companies are facilitating espionage or ever acted

---

<sup>51</sup> *Kurtis J. Kintzel*, Order to Show Cause and Notice of Opportunity for Hearing, 22 FCC Rcd 17197, 17207, ¶ 28 (2007); *NOS Communications, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6952, 6965, ¶ 28 (2003); *Business Options, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6881, 6894, ¶ 37 (2003); *Publix Network Corporation, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 17 FCC Rcd 11487, 11508, ¶ 47 (2002) (“*Publix Order*”); *CCN, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 12 FCC Rcd 8547, 8561, ¶ 24 (1997).

<sup>52</sup> *Order* at ¶ 1.

at the direction of the Chinese government, and having failed to discover any such evidence, the Commission continues to rely entirely on inferences about the Companies' ownership and the actions of other companies, and impermissibly shifted the burden to the Companies to prove their innocence.

- While inviting comment, the *Order* mistakenly applies a preponderance of the evidence standard that it claims is “well-established in the absence of any statutory requirement to the contrary,” relying entirely on the decision of the Supreme Court in *Steadman v. SEC*.<sup>53</sup> The *Order*'s reliance on *Steadman* is misplaced. Here, the more appropriate standard is the “clear and convincing evidence” standard that the Commission itself applied in *Sea Island Broadcasting*, where the Court of Appeals for the District of Columbia Circuit concluded that “revocation of an FCC license is governed, at the agency level, by the ‘clear and convincing’ standard of proof set forth in the *Collins* decision for an SEC revocation of a broker’s license.”<sup>54</sup> That *Steadman* was decided a year later does not change this particular standard for revocation especially where, as here, revocation would destroy the Companies’ livelihood in the U.S. that was established under permanent Section 214 authorizations. As has been noted since *Steadman*, the clear and convincing standard continues to apply when a defendant in an administrative proceeding faces a judgment that “could potentially impose penalties such as loss of liberty, deportation, termination of parental rights, or *deprivation of ability to*

---

<sup>53</sup> *Id.* n.52 (citing *Steadman v. SEC*, 450 U.S. 91, 101 & n. 21 (1981)).

<sup>54</sup> *Sea Island Broadcasting v. FCC*, 627 F.2d 240, 244 (D.C. Cir. 1980).

*engage in one's livelihood.*"<sup>55</sup> In this case, the Commission is seeking to permanently bar the Companies from being able to provide Section 214 services. Importantly, *Sea Island Broadcasting* held renewable licenses and could hold or acquire other broadcast licenses.<sup>56</sup> If the Commission applied the "clear and convincing" standard in *Sea Island Broadcasting* based on those consequences, it certainly must do so here where the jeopardy is even greater.

- The *Order* repeatedly claims that this case does not "turn on any disputed facts," or that there are "no material facts in dispute."<sup>57</sup> As shown below, there is a list of material facts in dispute in this case. Indeed, the Commission's case, to the extent it is not based on unwarranted inferences, is based on material facts in dispute.
- The Commission's precedent demonstrates that it has typically reserved revocation of a license or authorization for a narrow set of cases involving serious misconduct or abuse.<sup>58</sup> In rejecting this precedent, the *Order* does not cite any contrary interpretation, aside from a different recent case involving a state-owned Chinese company. Rather, the Commission simply asserts, notwithstanding its past precedent, that it is now "unreasonable" to conclude serious misconduct could be the only reason for revocation,

---

<sup>55</sup> *SEC v. Moran*, 922 F. Supp. 867 (S.D.N.Y. 1996) (emphasis added).

<sup>56</sup> *See Sea Island*, 627 F.2d at 243.

<sup>57</sup> *Order* at ¶¶ 14, 18, and 19.

<sup>58</sup> *See* OSC Response at 19; *Section 214 Entry and Exit Requirements*, Report and Order and Second Memorandum Opinion and Order, 14 FCC Rcd 11364, 11374, ¶ 16 (1999) (stating when adopting blanket domestic Section 214 authorizations "the Commission will still be able to revoke a carrier's section 214 authority when warranted in the relatively rare instances in which carriers abuse their market power or their common carrier obligations").

and fails to provide any limiting principle, instead stating the rather broad rule that it must evaluate “all aspects of the public interest.”<sup>59</sup>

- Notwithstanding the seriousness of the charges and the extensive list of material facts in dispute provided below, the *Order* refuses to afford the Companies the opportunity of a hearing. The *Order* simply states that even if the Commission had required hearings for Section 214 revocations, “we no longer believe that such a policy is appropriate,” citing to national security concerns.<sup>60</sup> The Commission has thus expressed its willingness to abandon normal procedural protections as it considers a specific enforcement matter.
- Notwithstanding the *Order*’s repeated “deference” to the authority of the Executive Branch agencies on matters of national security,<sup>61</sup> the Bureau provided them no more than 30 days from October to November, 2020 to respond to the Companies’ OSC Response and provide supporting documentation to the Commission.<sup>62</sup> This, despite the Commission having received the OSC Response in June, 2020. And, as noted above, while the Executive Branch Agencies Letter does speculate about various possible risks, the Executive Branch agencies then declined to make a specific recommendation to the Commission, “[g]iven the nature of the Commission’s request for views on discreet factual questions, and the limited time allotted for response.”<sup>63</sup>

---

<sup>59</sup> *Order* at ¶ 21.

<sup>60</sup> *Id.* at ¶ 17.

<sup>61</sup> *See id.* at ¶¶ 4, 23 and 69.

<sup>62</sup> *See* Bureau Request Letter at 1.

<sup>63</sup> *See* Executive Branch Agencies Letter at 1.



- The OSC Response showed that the questions at issue in this proceeding are serious and extensive enough to warrant a rulemaking proceeding to ensure that the new procedural and substantive requirements applicable to all Section 214 holders could be comprehensively reviewed to avoid inconsistent enforcement and protect against violations of due process.<sup>64</sup> Yet, the Commission waved these questions away, simply reiterating its “very broad discretion” to proceed by adjudication or rulemaking.<sup>65</sup> It refused to engage the question of whether a rulemaking would better protect the rights of the Companies and other Section 214 authorization holders, instead stating, without explanation, its belief that the issues raised here are best resolved through “party-specific procedures.”<sup>66</sup>
- Notwithstanding years of Team Telecom using security agreements to minimize national security risks, the Commission brushes aside any possibility of mitigation.<sup>67</sup>

In sum, then, the Commission shifted the burden of proof, chose a less stringent burden for itself than the law requires, refused to acknowledge that material facts are in dispute when they clearly are in dispute, expanded the grounds justifying revocation to the point where there is now no reasonable constraint on the Commission’s revocation powers, refused to hold a hearing, refused to provide the expert agencies sufficient time for input, proceeded without a recommendation from those expert agencies, refused to review any of the procedural or

---

<sup>64</sup> OSC Response at ¶¶ 27-30.

<sup>65</sup> *Order* at ¶ 21.

<sup>66</sup> *Id.*

<sup>67</sup> *Id.* at ¶¶ 67-69.

substantive questions raised by this extraordinary process in a rulemaking, and refused to conduct any analysis as to whether any of the risks it has identified could be mitigated.

The overall impression is that the Commission is willing to ignore or reverse any possible procedural or evidentiary constraint to reach a pre-ordained conclusion. The *Order* asks whether a hearing is warranted, and goes on at length about the Commission’s discretion. But the point is not that in certain circumstances the Commission may have the discretion to choose different ways of proceeding. The point is that the way the Commission *has* chosen to proceed here fails to provide the Companies the kind of protections consistently applied in past revocation proceedings. The Commission’s desire to oust the Companies from the U.S. market cannot justify procedural shortcuts where, as here, the consequences to the Companies are so severe.

**B. The *Order* Improperly Avoids an Evidentiary Hearing**

In the aggregate, the above list shows that the Commission has, effectively, already decided the outcome it wishes to have and has crafted the process so as to avoid considering any facts warranting a different outcome. Given the nature of the interests at stake and the inferential nature of most of the evidence so far, it is particularly egregious for the *Order* to deny a hearing before a neutral finder of fact like an Administrative Law Judge.

The Commission states that the Section 214 revocations identified by the Companies as being designated for hearing in the past are only indicative of the Commission’s determination that such proceedings were worthy of a hearing because that was the best measure for “the proper dispatch of business and to the ends of justice.”<sup>68</sup> It is thus surprising that the Commission should be so resistant to the idea of a hearing here. Why should the same logic

---

<sup>68</sup> See *id.* at ¶ 16.

applied to past revocation proceedings not extend to the present instance? Are the “ends of justice” different in this instance? The *Order* fails to compare the circumstances of these different cases to explain its position.

The *Order* goes on to state that even if those cases represented a past policy, such policy is no longer appropriate, citing to the Supreme Court’s finding in *Mathews v. Eldridge* that “the ordinary principle [is] that something less than an evidentiary hearing is sufficient prior to adverse administrative action.”<sup>69</sup> Of course, the Commission cases occurred well after *Mathews* was decided, and the Commission nevertheless held hearings. Moreover, there is nothing ordinary about this proceeding. This is essentially the same, unprecedented proceeding that has been applied contemporaneously to a small group of Section 214 holders. The Commission has not asserted any material violation of the Commission’s rules to precipitate the present proceeding. Rather, the Commission relies on sudden concerns about national security, new in the 12 years since Pacific Networks acquired ComNet and, allegedly, utterly unable to be mitigated. “Ordinary” principles were passed the moment the Commission commenced this proceeding, and left well behind when the *Order* concluded, unilaterally, that there are “no substantial and material questions of fact.”<sup>70</sup>

That the *Order* should have taken this turn is particularly surprising given that only recently, in 2020, the Commission explained in the Administrative Hearings Order when due process requires an evidentiary hearing, and in such instances applying the three-part test the

---

<sup>69</sup> *Mathews v. Eldridge*, 424 U.S. 319, 343 (1976).

<sup>70</sup> *Order* at ¶ 19.

Supreme Court adopted in *Mathews*.<sup>71</sup> These factors weigh in favor of providing the Companies with a live hearing, though remarkably the *Order* does not substantively apply the three-part test.

According to the three-part test, the Commission must consider (1) “the private interest that will be affected by the official action,” (2) “the risk of erroneous deprivation of such interest through the procedures used as well as the probable value, if any, of additional or substitute procedural safeguards,” and (3) “the Government’s interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirements would entail.”<sup>72</sup>

Under the first part, revocation of the Companies’ Section 214 authorization would eliminate the Companies’ ability to continue to provide telecommunications services to customers in the U.S. on a common carrier basis. The Companies have built a business that provides service to hundreds of thousands of users of retail calling cards, millions of minutes of carriage to service providers using Wholesale IDD, and efficient intracompany communications to companies using MPLS VPN. Revocation of the Companies’ authorization would cripple their businesses and likely result in employees in the U.S. losing their jobs at a time of considerable economic uncertainty. And the damage to the reputation of the Companies and their employees should not be ignored: officially branding any company as a risk to national security would permanently stain the reputation of the Companies and their employees. The

---

<sup>71</sup> *Procedural Streamlining of Administrative Hearings, Report and Order*, 35 FCC Rcd 10729, 10733, ¶ 12 (2020) (“[t]o determine whether due process requires live testimony is a particular case, the presiding officer will apply the three-part test the Supreme Court adopted in *Mathews v. Eldridge*”); see also, *Mathews v. Eldridge*, 424 U.S. at 335.

<sup>72</sup> *Mathews v. Eldridge*, 424 U.S. at 335.

impact of a revocation on the interests of the Companies and its employees are thus extensive and weigh heavily in favor of a neutral finder of fact reviewing the record.

Under the second part, a balance of the risk of erroneous deprivation of these interests through the *Order*'s procedures and the probable value of the procedural safeguards provided by a hearing weighs heavily in favor of a hearing. The clear intent of this directive is to consider providing more process, not less. The *Order*'s "factual conclusions" on the written record to date still rely almost entirely on hypotheticals, inference, and potential implications rather than factual evidence. As noted above, the *Order* made unwarranted conclusions about the Companies' transparency without the Commission having sought clarification, and did not even correctly characterize the one service that it did analyze. All of this shows that the risk of "erroneous deprivation" is and will continue to be significant and merits "additional or substitute procedural safeguards" to evaluate material facts, not "further proceedings" that simply continue to limit the Companies' procedural protections.

Under the third part, the *Order* does not provide a coherent explanation as to how the fiscal or administrative burdens would outweigh the other two parts. To be sure, the *Order* rather vaguely states that the "fiscal and administrative burden of such additional process *could* be quite substantial and disruptive if it were to involve participation by Commission staff or officials from other agencies in oral proceedings."<sup>73</sup> By this statement, however, the *Order* acknowledges the extent of participation needed in this proceeding to reach a fair conclusion, leading to the conclusion that multiple sources could weigh in on material facts at issue in this case. But importantly, the *Mathews* test does not allow an agency to ignore the need for a

---

<sup>73</sup> *Id.* at ¶ 17 (emphasis added).

hearing based on the existence of *any* burden more significant than that of the current process. So simply pointing to the possibility of added expense or burden is not enough—the *Order* must, and fails, to show that the burden is disproportionate to the need for a hearing as demonstrated by the first two parts. To the extent the Commission attempts to rely on an opinion or statement regarding disputed issues of material fact—and there is an entire list of them below—such opinion or statement should be subject to review and dispute by the Companies using substantiated evidence. An oral proceeding is necessary to ensure that the Companies are presented with the evidence held against them and have an adequate opportunity to rebut it. This is particularly important here, given the substantial private interests at stake and the weaknesses of the unprecedented process as implemented thus far.

Not only would the *Mathews* test, had it been properly applied by the *Order*, make clear a hearing is warranted, but Commission precedent does as well. Historically, the Commission has only revoked Section 214 authorizations without holding an evidentiary hearing in cases where the respondent has failed to respond to notices from the Commission. In those limited instances, that companies had failed to respond to multiple inquiries from the Commission and had presumably gone out of business, making a hearing unnecessary.<sup>74</sup> Absent those unusual circumstances, and as explained in the OSC Response, the Commission designated Section 214 authorizations for hearing and provided the respondent an opportunity to be heard.<sup>75</sup> The hearing

---

<sup>74</sup> See, e.g., *Wypoint Telecom, Inc. Termination of International Section 214 Authorization*, Order, 30 FCC Rcd 13431, 13432-33, ¶ 4 (IB 2015); *LDC Telecommunications, Inc.*, Revocation Order, 31 FCC Rcd 11661, 11662 ¶ 5 (EB, IB & WBC 2016) (revoking domestic and international Section 214 authorizations for failure to pay regulatory fees after carrier failed to respond to order to show cause); *WX Communications Ltd. Termination of International Section 214 Authorization*, Order, 34 FCC Rcd 1028, 1029-30, ¶ 5 (IB 2019).

<sup>75</sup> OSC Response at 36-37.

was not a mere formality in those circumstances, but rather provided the respondent an opportunity to raise specific evidentiary questions and to be heard by an unbiased arbitrator of fact.

The Commission must provide a reasoned justification for changing positions on existing policies. It is not sufficient to simply state that the Commission has changed its mind with regard to the revocation process.<sup>76</sup> The Commission cites to “relevant national security issues” and “public interest” as warranting a prompt response,<sup>77</sup> notwithstanding that this particular process has lasted over a year and could have been well down the road towards a full hearing by now. Those same complex, important concerns are all the more reason to ensure a thorough investigation and opportunity to be heard before an Administrative Law Judge.

### **C. The *Order*’s Process Conflicts with the Administrative Procedure Act**

Under the Administrative Procedure Act (“APA”), a reviewing court may set aside agency actions, findings, and conclusions when they are “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.”<sup>78</sup> As described above, the *Order* relies on several exercises of discretion and conclusions to remove procedural protections that would normally apply in a revocation case.

---

<sup>76</sup> See *Encino Motorcars, LLC v. Navarro*, 136 S. Ct. 2117, 2125-26 (2016) (“Agencies are free to change their existing policies as long as they provide a reasoned explanation for the change. . . . [T]he agency must at least ‘display awareness that it is changing position’ and ‘show that there are good reasons for the new policy.’”) (quoting *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009)).

<sup>77</sup> See *Order* at ¶ 17.

<sup>78</sup> 5 U.S.C. § 706(2)(A); *United States v. Bean*, 537 U.S. 71, 77 (2002).

The scope of review under the APA is narrow, and a court may not substitute its judgment for that of the agency,<sup>79</sup> though the agency must demonstrate that it engaged in reasoned decision-making.<sup>80</sup> Moreover, the Supreme Court has restricted review of agency action for abuse of discretion when the authorizing statute is “drawn in such broad terms that in a given case there is no law to apply.”<sup>81</sup>

In the present case, should the Commission decide to proceed as intended under the *Order*, its process would likely be set aside as impermissibly arbitrary, capricious and an abuse of discretion. The list of unilateral and unannounced changes to policy the Commission has had to adopt within this adjudicatory proceeding—in some cases with little to no reasoned discussion—is substantial, and the Commission will be put in the position of having to defend each one of those decisions, both individually and in the aggregate effect they have on the overall fairness of this proceeding. Moreover, the Commission will be unable to rely on the exception to APA review provided for abuses of discretion, given that the *Mathews* test—which the Commission failed to apply contrary to its own recent procedural order—provides a clear test for when an exercise of discretion is warranted and not warranted. Separately, while the Commission is admittedly given broad latitude to decide between proceeding by rulemaking and proceeding by adjudication, the Commission’s bare minimum justification for continuing this process without a comprehensive rulemaking, despite the extensive unanswered questions raised

---

<sup>79</sup> *Motor Vehicle Manufacturers Ass’n v. State Farm Auto Mutual Insurance Co.*, 463 U.S. 29, 43 (1983) (“*State Farm*”).

<sup>80</sup> *Id.*, 463 U.S. at 52.

<sup>81</sup> *Citizens to Preserve Overton Park v. Volpe*, 401 U.S. 402, 410 (1971).



by this extraordinary process,<sup>82</sup> is reasonably viewed as crossing outside the boundary of the agency’s discretion.

**D. The *Order*’s Process Conflicts with the Due Process Clause**

The Companies’ Section 214 authorizations are a protected interest, as the Companies had a reasonable expectation that absent material changes in the authorization, the authorization would continue to be effective indefinitely.<sup>83</sup> For Section 214 authorizations, the Commission’s discretion to revoke the authorization lies only in cases of adjudicated misconduct.<sup>84</sup> “Adjudicated misconduct” is defined as “a violation of the terms of an authorization, the [Communications] Act, or a Commission rule or order.”<sup>85</sup> Yet, the *Order*’s identification of national security concerns is founded on hypotheticals and presuppositions that are not based on any evidence of actual misdeeds by the Companies.

Moreover, the *Order*’s process prejudices the Companies by denying them an opportunity to be heard and “fair processing of an action.”<sup>86</sup> The Companies are prejudiced by the Commission’s failure to administer its rules in a consistent fashion and provide the Companies’ with a full and fair hearing before a neutral arbitrator.

---

<sup>82</sup> See OSC Response at 27-30.

<sup>83</sup> See, e.g., *Spinelli v. New York*, 579 F.3d 130, 168-69 (2009) (holding that a granted business license is a protected property interest requiring due process); see also, *3883 Conn. LLC v. Dist. of Columbia*, 336 F.3d 1068, 1072 (D.C. Cir. 2003).

<sup>84</sup> See *Foreign Participation Order*, 12 FCC Rcd 23891, 24022, at ¶ 295 (1997).

<sup>85</sup> See *Marpin Telecoms and Broadcasting Co. Ltd. v. Cable & Wireless, Inc.*, 18 FCC Rcd. 508, 515 (2003).

<sup>86</sup> See *United States v. Morgan*, 193 F.3d 252, 267 (1999) (quoting *Garcia-Flores*, 17 I. & N. Dec. 325, 329 (BIA 1980)).

As a protectable interest, the U.S. Constitution requires “basic fairness” and “procedures reasonably designed to protect against erroneous deprivation of” a party’s interests.<sup>87</sup> Due process in the present circumstances warrants a hearing before the Companies are deprived of their protectable interests in the Section 214 authorization.<sup>88</sup> The Commission asserts that a hearing “would serve little purpose here,” as the Commission “intend(s) to base any revocation or termination solely on evidence that has already been introduced or that can be introduced in subsequent written pleadings.”<sup>89</sup>

Yet, the record of this proceeding shows numerous facts clearly material to a revocation decision that are in dispute, and require adjudication by a neutral finder of fact:

- The core assertion of the *Order* is that the Companies are subject to the exploitation, influence and control of the Chinese government. The Companies have disputed this in the OSC Response and dispute this assertion further in this response.<sup>90</sup> The Commission has not shown any example of the Companies taking any inappropriate actions as a result of direction from the Chinese government, and the Company has certified under penalty of perjury that “[a]t no time have any officials of the government of the People’s Republic of China or of the Chinese Communist Party directed or requested that Pacific Networks or ComNet take or refrain from taking any particular action.”<sup>91</sup> Notably, the *Order* spends paragraphs asserting

---

<sup>87</sup> *Al Haramain Islamic Found, Inc. v. U.S. Dep’t of Treasury*, 686 F.3d 965, 980 (9<sup>th</sup> Cir. 2012).

<sup>88</sup> *See, e.g., Zinermon v. Burch*, 494 U.S. 113, 132 (1990) (requiring a predeprivation hearing where feasible).

<sup>89</sup> *See Order* at ¶ 18.

<sup>90</sup> OSC Response at 19-22.

<sup>91</sup> *Id.*, Declaration of Li Ying (Linda) Peng (“Declaration”).

and reiterating that the Companies are subject to a significant degree of control by their Chinese indirect owners. Clearly, the facts relevant to making any reliable determination on this particular, crucial matter are in dispute. It is incredible to assert otherwise.

- The next link in the Commission’s chain of inferences is that because the Companies are subject to the control of the Chinese government, they necessarily raise not just “significant national security and law enforcement risks” but “pose a clear and imminent threat to the security of the United States due to Pacific Networks’ and ComNet’s access to U.S. telecommunications infrastructure.”<sup>92</sup> As noted above, the *Order* does not provide any detailed explanation of exactly how such a threat might be carried out as a result of the Companies’ Section 214 authorizations, instead citing the Executive Branch agencies’ assumption that any connection to any telecommunications networks somehow creates such a threat. The *Order* does not explain how ComNet’s Wholesale IDD or Retail Calling Card services could be used to pose the threat it alleges and concludes that Pacific Networks’ MPLS VPN service is particularly worrisome because of its use of BGP servers to peer with other providers,<sup>93</sup> notwithstanding the fact that Pacific Networks does not use its routers in this way. Notably, the Commission does not limit its assertions to the Companies’ services authorized under Section 214, but also cites to VoIP, which the Commission does not regulate as a common carrier service, and as such could be provided by the Companies without a Section 214 authorization. Again, the basis for the Commission’s assertion that the

---

<sup>92</sup> *Order* at ¶ 22.

<sup>93</sup> *Id.* at ¶ 45.

Companies, through their Section 214 services, pose any particular significant threat to the U.S. is in material dispute.

- Related to this point, the record of the *China Telecom* proceeding shows that the Internet Governance Project at the Georgia Institute of Technology commented and filed an *ex parte* statement raising questions as to whether alleged misrouting by China Telecom amounted to malicious hijacking.<sup>94</sup> Since the *Order* asserts the Companies could engage in the same behavior, the basis for whether this type of conduct amounts to a real or imagined security threat engaged in by other Chinese companies is a material fact in dispute.
- The *Order* does assert that, because of the Companies’ Section 214 services, they have access to personally identifiable information and CPNI.<sup>95</sup> The Companies dispute, however, that they ever have or ever would violate the law of the United States or their own data privacy policies, provided in response to Question 12 below, as well as the laws of the United States, by misusing access to such data.
- Similarly, the *Order* questions whether the Companies can be trusted to “cooperate with the U.S. government” regarding CALEA interception requests and hold in confidence the fact that such requests have been received.<sup>96</sup> [REDACTED]

---

<sup>94</sup> See Comments of the Internet Governance Project, Georgia Institute of Technology’s School of Public Policy, GN Docket No. 20-109 (filed Dec. 17, 2020); Ex Parte Comments of the Internet Governance Project, Georgia Institute of Technology’s School of Public Policy, GN Docket No. 20-109 (filed Mar 8, 2021).

<sup>95</sup> *Order* at ¶ 51.

<sup>96</sup> *Id.*

[REDACTED]

[REDACTED]<sup>97</sup>

- The *Order* asserts that there are discrepancies among statements made by the Companies to the Senate Subcommittee leading to the PSI Report on one hand and statements to Team Telecom and the Commission on the other about the degree of control exercised over the Companies by indirect owners and the location of and access to databases, and further asserts that the Companies omitted material information they should have provided to the Commission when responding to the *OSC*. The Companies fully rebut these assertions herein and in the answer to Question 19, below. This rebuttal makes clear that there are material disputes of fact as to whether (1) there were any discrepancies at all, (2) the location of databases abroad and restricted access by support staff constitutes any sort of violation of the 2009 Letter of Assurance or raises any material security or privacy risk, (3) the Companies' security and access policies are sufficient to protect customer records, (4) promulgation of data security policies by CITIC Tel constitutes material involvement in the Companies' day-to-day management contrary to the Companies' statements, (5) the Companies omitted material information in the *OSC* Response, and (6) assuming *arguendo* there was any omission, that the omission was willful, much less intentional and knowing.
- Related to this, the Companies have never seen documents cited by the PSI Report, and which the *Order* also cites.<sup>98</sup> These documents may be nothing more than presentations or summaries provided by the Companies to the Senate Subcommittee, or they may be some

---

<sup>97</sup> *OSC* Response at 20.

<sup>98</sup> See, e.g., *Order* nn.130, 131, 132, 238, 246, 259, 263, 264.

third-party document. The Companies have no way of knowing. Thus, contrary to the *Order's* assertion that the Companies have access to all of the materials they need, and that discovery is not necessary, the Companies in fact have not had access to materials cited in the PSI Report that have now been relied on by the Commission.

- The *Order* dismisses the Companies' explanation of the limited application of certain Chinese laws to them and their U.S. operations, and continues to make broad assertions that Chinese law exerts a coercive effect on the Companies that would overcome any obligation to obey U.S. law.<sup>99</sup> As discussed above, the coercive effect of Chinese law on U.S. corporations and their U.S.-located operations is in dispute.
- The *Order* repeatedly states that there is no possible mitigation of the risks posed by the Companies.<sup>100</sup> The Companies explain herein how the *Order* itself shows that a variety of measures could substantially reduce possible risks. Whether additional mitigation measures could address security risks is thus also a material fact in dispute.

The above facts are not incidental to the *Order's* decisions—they are repeatedly cited as the core chain of reasoning and justification for revoking the Companies' authorizations. It is impossible to maintain that they are neither material nor in dispute. The question, then, is not whether the Commission *could* conduct this process without a hearing, but whether it *must*, and whether its failure to do so ultimately amounts to a denial of due process.

Given the number, scope and importance of the facts at issue, it is crucial that this proceeding allow a neutral finder of fact exercising adjudicatory authority, an opportunity for the

---

<sup>99</sup> *Order* at ¶ 37-39.

<sup>100</sup> *Id.* at ¶¶ 22, 67-69.

Companies to provide materials and an opportunity for Companies to view evidentiary information reviewed by the Commission.

**E. The *Order*'s Assertion that the Commission Can Serve as a Neutral Fact Finder is Unavailing**

The *Order* asserts that a hearing before an Administrative Law Judge is not necessary because any decision could be appealed to the Commission, and because the Companies have not “[a]rticulated any particularized and compelling reason why the Commission or any individual Commissioner would not be able to serve as a neutral decisionmaker in this matter.”<sup>101</sup> As discussed in detail in this response, however, the *Order* itself shows a willingness to interpret every fact against the Companies, and to ignore every piece of evidence of the Companies’ compliance with Commission regulations and the 2009 Letter of Assurance. The Commission took no opportunity over the ten months that it had the OSC Response to reach out to the Companies and clarify any of the alleged discrepancies or omissions, instead reserving them to bolster its case for revocation. The results from other similar cases also indicate an unwillingness on the part of the Commission to consider any mitigating facts contrary to its narrative.<sup>102</sup> In this case, the Commission is acting as the investigator, prosecutor and finder of fact. Where relevant facts are readily apparent—a licensee has gone out of business, for example—then this kind of inquisitorial process is allowed for the sake of administrative expediency. But where there are as many facts in dispute as there are in this case, it should be a

---

<sup>101</sup> *Id.* at ¶ 20.

<sup>102</sup> *See, e.g.*, Reply Comments of China Telecom (Americas) Corporation to Order Instituting Proceedings, GN Docket No. 20-109 (filed Mar. 1, 2021) at 2-3.

given that the facts will be reviewed by a neutral fact finder that has not interpreted every fact against the Companies.

#### **IV. RESPONSES TO QUESTIONS**

1. An identification of the Chinese government entity that owns and controls CITIC Group Corporation and the ownership interests held by such entity in CITIC Group Corporation.

The Ministry of Finance of the People's Republic of China owns 100% of the equity interests in CITIC Group Corporation.

2. A detailed description of the management and oversight of Pacific Networks and ComNet by any entity that holds a ten percent or greater direct or indirect ownership interest in and/or controls Pacific Networks and ComNet.

As the Companies stated in the OSC Response, CITIC Tel is the only entity holding a ten percent or greater direct or indirect ownership interest in the Companies that exercises any degree of management and oversight over the Companies.

On an annual basis, the Companies submit to CITIC Tel their Annual Operating Plan ("AOP") detailing their budgets, revenue and operating expenditures for the upcoming three years, together with the forecasted actual numbers of the current year. The AOP is prepared by each Company to show material variances between the budgeted and forecasted actual, which are then discussed with CITIC Tel. The AOP serves as the key financial performance indicator for the Companies. Monthly financial information is reported to CITIC Tel for group consolidation purposes and the Companies' local management team will explain any material variation from the AOP. As part of the oversight of the Companies' financial positions, CITIC Tel has provided guidance to the Companies from time to time regarding changes in accounting standards or specific accounting issues as they may arise.



Periodically, CITIC Tel’s internal and external auditors will perform IT governance audits of the Companies, as part of larger audits of the operations of CITIC Tel and its subsidiaries. Related to financial matters, CITIC Tel’s internal and external auditors also perform periodic audits on the Companies’ treasury processes, cash management process, fixed assets management process, human resources process, inventory management process, credit control, financial system, risk management, and financial reporting. Any findings, together with remediation actions, are discussed and agreed with the Companies and reported to the executive directors of CITIC Tel.

As detailed above and in response to Questions 6, 7 and 9, CITIC Tel has adopted policies related to information technology, security and access that have been shared with the Companies. The Companies are expected to implement their own policies and controls with reference to those guidelines. This fact, however, has been long known to the United States government, since the Companies provided a full set of the applicable policies in 2009 to Team Telecom as required by the 2009 Letter of Assurance. This policy was titled the “Pacific Networks Corp. IT Security Policy,” but was derived from the then current CITIC Tel Information Technology Security Policy. As the *Order* notes, [REDACTED]

[REDACTED]

[REDACTED]<sup>103</sup>

As the *Order* states,<sup>104</sup> the directors of Pacific Networks and ComNet (the “Directors”) are also executive directors of CITIC Tel. Specific approval by the Directors is required for

---

<sup>103</sup> *Order* at ¶ 27.

<sup>104</sup> *Id.* at ¶ 34.

opening and closing bank accounts, changes in bank signatories and other significant financial matters (such as mergers, acquisitions etc.). Directors' decisions are not, however, required for the Companies to carry out their day-to-day responsibilities. The Companies estimate that involvement of the Directors in oversight and management of the Companies' operations occupy an insignificant amount of their time.

No indirect owner of the Companies other than CITIC Tel has exercised any management or control over either of the Companies.

3. An identification of all officers, directors, and other senior management of all entities that hold a ten percent or greater direct or indirect ownership interest in and/or control Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government.

The Companies refer the Commission to the information provided in the OSC Response.<sup>105</sup> Further, information about the officers, directors and other senior management of the following entities that hold a ten percent or greater ownership interest in and/or control Pacific Networks and ComNet is provided as follows:

CITIC Telecom International Holdings Limited ("CITIC Tel")

A list of CITIC Tel's directors and corporate management, together with biographies for each of them, can be found at <https://www.citictel.com/about-us/leadership/>.

CITIC Limited

A list of CITIC Limited's directors, senior management and management, together with biographies for each of them, can be found at [https://www.citic.com/en/aboutus/board\\_of](https://www.citic.com/en/aboutus/board_of)

---

<sup>105</sup> OSC Response at 11-12, Exhibits A, B and C.

[directors/](#), [https://www.citic.com/en/aboutus/senior\\_management/](https://www.citic.com/en/aboutus/senior_management/) and <https://www.citic.com/en/aboutus/management/>.

#### CITIC Group

A list of the members of CITIC Group’s Group Party Committee, Board of Directors, Board of Supervisors, and Senior Management, together with biographies for each of them, can be found at [https://www.group.citic.com/en/About\\_CITIC/Directors\\_Senior/](https://www.group.citic.com/en/About_CITIC/Directors_Senior/).

4. A clarification whether ComNet is an LLC or a corporation as represented in certain filings before the Commission and, if necessary, explain in detail when a legal change occurred and whether Commission notification was required.

ComNet was formed as a limited liability company (“LLC”) in 1999. It has remained an LLC, and thus there has been no legal change that would have required Commission notification.<sup>106</sup> The 1999 and 2009 statements cited in the *Order* that ComNet is a “corporation” appear to have been inadvertent misstatements.

5. A description and copy of any policies or agreements concerning Pacific Networks’ and ComNet’s corporate governance or decision making.

Attached as Exhibit A are (1) the Articles of Incorporation and Bylaws for Pacific Networks and (2) the current limited liability company agreement for ComNet. These documents are comparable to the governing documents of other U.S. corporations and limited liability companies, and would be considered “policies or agreements” concerning the Companies’ corporate governance or decision making. As these documents are typical of

---

<sup>106</sup> As stated in the OSC Response, ComNet did change its name from CM Tel (USA) LLC to its present name in 2010. *Id.* at 6. This change was notified to the Commission and noticed by it. *International Authorizations Granted; Section 214 Applications (47 C.F.R. § 63.18); Section 310(b)(4) Requests*, File No. ITC-214-20090424-00199, Public Notice, DA 10-499, 25 FCC Rcd 2838, 2841-42 (2010).

organizational documents for corporations and LLCs, they do provide for the management of the business by their respective Directors. However, as is also often the case for corporations and LLCs, the Directors of both Companies have delegated day-to-day responsibility for management except for involvement in certain significant financial decisions, and, as stated in response to Questions 2 and 19, spend an insignificant amount of their time involved in the Companies' management and operation.

6. With respect to U.S. customer records, provide: (1) an identification and description of the location(s) where U.S. customer records are stored, including original records, back-up records, and copies of original records; (2) a description and copy of any policies or agreements governing access to U.S. customer records; (3) an explanation and identification as to which entities and individuals have access to U.S. customer records, how such access is granted, and any corporate policies concerning such access.

Customer records for different types of service are handled differently. The following describes how U.S. records are handled for ComNet's Wholesale IDD service, ComNet's Retail Calling Card service, and Pacific Networks' MPLS VPN service, and provides information regarding the storage of VoIP service records.

Wholesale IDD Service

- (1) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED]

(2) Access to these U.S. customer records is governed by Section 10 of the current version of the CITIC Tel Information Security Policy, attached hereto as Exhibit B.<sup>107</sup>

(3) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] For this service, access to records is coordinated by CITIC Tel according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy.

#### Retail Calling Card Service

(1) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] No copies are stored outside of U.S.

(2) Access to these U.S. customer records is governed by Section 10 of the current version of the CITIC Tel Information Security Policy, attached hereto as Exhibit B.

---

<sup>107</sup> This is the current version of the policy provided to Team Telecom in 2017 and included in Exhibit K in the OSC Response.

(3) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] For this service, access to records is managed by ComNet according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy.

MPLS VPN Service

(1) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

(2) Access to these U.S. customer records is governed by Section 10 of the current version of the CITIC Tel Information Security Policy, attached hereto as Exhibit B.

(3) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]

[REDACTED] For this service, access to records is coordinated by [REDACTED]

[REDACTED] according to the corporate policy for granting such access detailed in Section 10 of the CITIC Tel Information Security Policy.

As explained in this response and also in response to Question 19, ComNet discussed the storage of VoIP service records with Senate Subcommittee staff, leading to the incorrect statement in the PSI Report that all of the Companies' service records are stored in the U.S. Originals, backups and copies of ComNet's VoIP records are only stored in the U.S., access is governed by Section 10 of the CITIC Tel Information Security Policy, and any access to such records by anyone located outside the U.S. must be authorized on an individual basis, as reported to the Senate Subcommittee staff at the time.

7. A description of who has access to the servers and/or data centers where U.S. customer records are located and any policies, agreements, or standards concerning access to the servers or data centers where U.S. customer records are stored.

Access to the data within the servers and/or data centers is addressed above in response to Question 6. The Companies understand this question to ask about physical access to the servers and/or data centers.

For [REDACTED]

[REDACTED] only authorized U.S. support engineers who have been registered in the data center access list can physically access the servers or tapes in secure rooms. Any physical access to the servers or tapes is recorded in logs maintained at [REDACTED]

[REDACTED]. Access rights to the servers and [REDACTED]

[REDACTED] are governed by Sections 6 and 10 of the current version of the CITIC Tel Information Security Policy, attached hereto as Exhibit B.

For the Wholesale IDD and MPLS VPN customer records stored in [REDACTED], only specifically authorized support engineers who have been registered in the data center access list can physically access the servers in secure rooms. Any physical access to the servers is recorded in logs maintained at the data center. Access rights to the servers and the [REDACTED] [REDACTED] are governed by Sections 6 and 10 of the current version of the CITIC Tel Information Security Policy, attached hereto as Exhibit B.

8. A detailed response as to whether any U.S. records are stored or were ever stored in CITIC Tel's data center in Hong Kong or in other non-U.S. locations, identifying the data center, its location, the time frame, and the type of service.

Please see the answer to Question 6. [REDACTED]

9. A detailed description of previous and present "practicable measures" taken to prevent unauthorized access to U.S. records as required by the 2009 LOA.

As noted in response to Questions 6 and 7, all access to U.S. records is governed by Sections 6 and 10 of the current version of the CITIC Tel Information Security Policy, attached hereto as Exhibit B. These policies are comparable to other corporate information security policies, and include the following protections:



- [REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]
- | [REDACTED]
- | [REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]  
[REDACTED]
- | [REDACTED]  
[REDACTED]

█ [REDACTED]

[REDACTED]

█ [REDACTED]

[REDACTED]

[REDACTED]

As described in response to Question 12, the Companies have implemented a CPNI policy in accordance with Commission rules.

10. A detailed description of what, if any, practicable measures Pacific Networks and ComNet have taken under the 2009 LOA to prevent unauthorized access if U.S. records are in fact stored in Hong Kong or other non-U.S. locations and accessible by their direct or indirect parent companies or other third parties.

Please see the response to Question 9. Records stored outside the U.S. that are accessible by personnel outside the U.S. are only accessible to individuals that have been granted access rights in accordance with the CITIC Tel Information Security Policy, and only if necessary to provide support to the Companies.

11. A detailed description as to whether Pacific Networks and ComNet failed to inform the Executive Branch agencies “of any material changes in any of the facts as represented in [the 2009 LOA], or in notices or descriptions submitted pursuant to this letter,” as required by the 2009 LOA.

As detailed in the *OSC Response*, the Companies have consistently informed Team Telecom of material changes, including changes to points of contact, ComNet’s name, ownership changes in 2012 and 2014 and, as noted above, the change in location of CITIC Tel’s servers.<sup>108</sup> The Companies are not aware of any failure to have informed Team Telecom “of any material

---

<sup>108</sup> OSC Response

changes in any of the facts as represented in [the 2009 LOA], or in notices or descriptions submitted pursuant to this letter.”

12. A description and copy of any policies and/or procedures in place to protect personally identifiable information (PII) and customer proprietary network information (CPNI).

Please see attached as Exhibit C the following policies and procedures:

- a copy of ComNet’s most recent CPNI filing, providing ComNet’s policies with regard to use of CPNI, obtaining customer approval for use of CPNI, notification of law enforcement of security breaches, and protections against disclosure of CPNI, including password authentication of customer contacts and immediate notification of password changes;
- a current copy of ComNet’s posted privacy policy applicable to calling card services at <https://www.comnet-telecom.us/privacy-policy>, detailing how ComNet, consistent with its CPNI policy, protects and may use personal data, and how the company obtains consent;

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

13. A description of any domestic interstate communications services that have been provided, are provided, and/or will be provided in the near future

Networks’ and ComNet’s blanket domestic section 214 authority as described in section 63.01 of the Commission’s rules, 47 CFR § 63.01.

Pacific Networks’ MPLS VPN service provides data communications that enable its customers to operate business applications among various customer sites both within the United States and internationally. To the extent this service makes use of domestic facilities and routes traffic within the U.S., the Companies consider it to also be provided pursuant to Pacific Networks’ blanket domestic 214 authority.<sup>109</sup>

Please note that for ComNet’s Retail Calling Card and Wholesale IDD services described in the OSC Response and at Question 14 below, these services are almost entirely used for international calls. It is possible, however, for the services to route U.S. domestic traffic, although this is a minimal amount of the traffic handled by the services. To the extent, then, that these services can facilitate domestic calls within the U.S. and a minimal amount of such calls are handled, the Companies consider these services to also be provided pursuant to ComNet’s blanket domestic 214 authority.<sup>110</sup>

---

<sup>109</sup> As noted in the OSC Response, the Department of Justice has stated that it “is unclear that an international Section 214 authorization is required” to provide MPLS VPN services. China Telecom (Americas) Corporation, Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate China Telecom’s International Section 214 Common Carrier Authorizations, File Nos. ITC-214-20010613-00346, ITC-214-20020716-0371, ITC-T/C20070725-00285 (filed Apr. 9, 2020) at 9. Accordingly, the Companies reserve and in no way waive the argument that the MPLS VPN services provided by Pacific Networks may not, in fact, require a Section 214 authorization.

<sup>110</sup> The OSC Response stated that these services were provided pursuant to the ComNet’s international section 214 authority, *see* OSC Response at 13-14, and while that is correct the Companies wish to be clear that the blanket domestic 214 authority would apply to the incidental amount of domestic traffic carried by the services.

14. A description of any services that have been provided, are provided, and/or will be provided in the near future pursuant to the international section 214 authorities granted to Pacific Networks and ComNet.

While Pacific Networks does not itself provide international circuits required for MPLS VPN, to the extent Pacific Networks' MPLS VPN service facilitates the exchange of international traffic, the Companies consider it to be provided pursuant to Pacific Networks' international Section 214 authority.

ComNet's Retail Calling Card service provides printed or digital phone cards with a set of 10-digit PIN numbers for international and domestic voice calls accessed via local or toll free numbers. As ComNet's Retail Calling Card service facilitates international calls, the Companies consider it to be provided pursuant to ComNet's international Section 214 authority.

ComNet's Wholesale International Direct Dial ("IDD") service handles international voice traffic and facilitates least cost routing for carriers located in the U.S. and in foreign locations. ComNet can provide this service through traditional TDM or through IP technology via SIP. The Companies consider this service to be provided pursuant to ComNet's international Section 214 authority.

15. A detailed description of Pacific Networks' and ComNet's domestic communications infrastructure within the United States and its connectivity to operations infrastructure within Hong Kong and China and provide a copy of what Pacific Networks and ComNet

provided to DOJ as identified in a June 8, 2018 letter from DOJ to Pacific Networks and ComNet.

Domestic Communications Infrastructure

In the OSC Response, the Companies provided an inventory of all equipment located in the U.S., and lists of all physical points of interconnection between Pacific Networks and ComNet and other carriers.<sup>111</sup> Those answers are incorporated herein by reference.

ComNet provides Wholesale IDD transit service facilitating both inbound and outbound voice traffic by interconnecting with U.S. carrier customers at ComNet's One Wilshire Building Data Center and then using VoIP SIP or T1/E1 TDM connections to route the traffic internationally.

ComNet provides Retail Calling Card service through its own calling card platform, which directly collects customer international direct dialed calls via direct inward dialing ("DID") numbers provided by local service providers, using VoIP SIP connections. End users can thus make international calls through the provided DID numbers by entering a 10-digit pin and destination number using their home or mobile phone.

ComNet serves as a VoIP service provider through a cloud-based PBX platform to enterprise users that offers the functions of an office telephone system without the need for the customer hosting a physical PBX in the office. The office users can make both domestic and international calls through ComNet's VoIP platform using their registered VoIP phones. This service is described in more detail below in response to Question 32.

---

<sup>111</sup> See *id.* at 15, 17, Exhibit D, G and H.

As stated in the OSC Response, ComNet also provides international Short Message Service (“SMS”), resells mobile SIM cards, and provides website development and hosting services.<sup>112</sup> These services do not require significant domestic communications facilities within the U.S. Please also note that while the OSC Response also stated that ComNet provided access to WeChat as part of its website service, ComNet ceased providing WeChat service later in 2020, following the issuance of an Executive Order prohibiting transactions related to WeChat.<sup>113</sup>

Pacific Networks’ MPLS VPN platform is located in data centers at 32 Avenue of the Americas in New York and One Wilshire, 624 Grand Avenue, Los Angeles, California in Los Angeles. Pacific Networks purchases [REDACTED]

[REDACTED] Pacific Networks also purchases from U.S. telecommunications carriers high-speed data connections from the New York and Los Angeles data centers to customer locations to facilitate provision of the service.

Pacific Networks leases [REDACTED] from U.S. facilities providers for sublease to [REDACTED] These circuits are used [REDACTED]

[REDACTED] Pacific Networks does not, however, provide any services over these circuits, have access to the traffic carried over the circuits, and they are not connected to Pacific Network’s points of presence or other locations.

---

<sup>112</sup> See *id.* at 14-15.

<sup>113</sup> *Addressing the Threat Posed by WeChat*, Executive Order 13943 (issued Aug. 6, 2020). The Companies provide an updated customer list for Website Service at Exhibit H hereto.

Connectivity to Hong Kong

CITIC Tel’s SOC in Hong Kong provides first tier support for ComNet’s Wholesale IDD service, Retail Calling Card service, International SMS Service and VoIP services. All access to ComNet’s systems through the SOC is governed by the CITIC Tel Information Security Policy, attached hereto as Exhibit B. Only the authorized monitoring system and engineer team in Hong Kong can monitor and manage the equipment in ComNet’s Los Angeles data center via MPLS VPN. As noted in response to Question 6, ComNet keeps a copy of its customer records in Hong Kong, which is also transferred via MPLS.

Separately, [REDACTED]  
[REDACTED] provides first tier support for Pacific Networks’ MPLS VPN service, and thus connects to the MPLS VPN service. All access to Pacific Networks’ systems through the [REDACTED]  
[REDACTED]<sup>114</sup> is governed by the CITIC Tel Information Security Policy, attached hereto as Exhibit B. Only the authorized monitoring system and engineer team in [REDACTED] can monitor and manage the equipment in Pacific Networks’ facilities via a private MPLS network. As noted in response to Question 6, Pacific Networks keeps a backup of its customer records in [REDACTED] which is also transferred via MPLS VPN.

---

<sup>114</sup> To be clear, this Network Operations Center that provides support to Pacific Networks is a different facility from the SOC that provides support to ComNet. The “NOC” identified in the PSI Report, *see* PSI Report at 96, is the CITIC Tel SOC identified above and distinguished from this facility.



### DoJ Presentation

Please see attached as Exhibit D the March 22, 2018 slide presentation provided to the Department of Justice during a site visit, as referenced in the June 8, 2018 letter.

16. A detailed response that explains: (1) what Autonomous System numbers have been assigned and deployed for the IP networks of Pacific Networks and ComNet; (2) whether Border Gateway Protocol (BGP) routers are used to exchange routing updates to forward IP traffic between these (i.e., Pacific Networks' and ComNet's) networks, or whether an Interior Gateway Protocol (IGP) routing protocol (e.g., OSPF or IS-IS) is used to forward IP traffic between these networks; and (3) if BGP is used, whether Pacific Networks and ComNet directly peer BGP speakers with no intermediate third party BGP routing provider connecting both networks.

### ComNet

(1) ComNet has been assigned and deployed Autonomous System number 14923.

(2) ComNet uses BGP routers to connect to the Internet through service providers [REDACTED]

[REDACTED] However, Pacific Networks and ComNet's networks are not connected, and thus IP traffic is not forwarded between these networks. ComNet has 5 class C subnets (203.160.32.0, 203.160.33.0, 203.160.35.0, 203.160.36.0 and 203.160.37.0) that are published through both the IPT service providers. Only static routes are deployed in ComNet's firewalls to forward IP traffic, with the firewalls managed solely by ComNet's Los Angeles engineers and no access allowed to engineers located outside the U.S.

(3) ComNet has no intermediate third party BGP routing provider.

### Pacific Networks

The *Order* states that "Pacific Networks' MPLS VPN service involves the use of Points of Presence to peer with other providers using Border Gateway Protocol (BGP) routers" and then notes that "the offering of IP Transit services in the form of using BGP is a prime candidate for

security exploitation.”<sup>115</sup> While Pacific Networks’ MPLS VPN does use BGP routers, the service is *not* an IP Transit service. As the Companies stated in the OSC Response, Pacific Networks’ MPLS VPN service provides data communications between and among customer sites within the U.S., and internationally, enabling the operation of business applications at those sites. The service does not provide IP Transit for Internet service. Moreover, as noted above, Pacific Networks and ComNet networks are not connected, so there are no BGP or IGP routers or routing protocols being used to exchange routing updates nor forward IP traffic between these networks.

Please note that, in the OSC Response, Pacific Networks listed two routers as being used for Pacific Networks services: [REDACTED]

[REDACTED].<sup>116</sup> On review, Pacific Networks has determined that neither of those routers are used by Pacific Networks to provide services and were listed by mistake. A revised list of equipment responsive to Question 6 of the OSC is attached hereto as Exhibit E.

In response to (1), Pacific Networks has deployed Autonomous System number 4058 for its MPLS VPN platform in its New York and Los Angeles data centers. This Autonomous System number is assigned to [REDACTED] that was disclosed to the Commission as a wholesale customer of Pacific Networks in the OSC Response.<sup>117</sup> Pacific Networks uses its wholesale customer’s Autonomous System number only for the purpose of interconnection with the U.S. telecommunication carriers that provide

---

<sup>115</sup> *Order* at ¶ 45 & n.219.

<sup>116</sup> OSC Response, Exhibit D.

<sup>117</sup> *Id.*, Exhibit E.

Pacific Networks the data connections used to reach U.S. customer locations, which then enables Pacific Network to provide connectivity to customer locations outside the U.S. served by the wholesale customer.

17. A detailed response that explains,

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

18. An identification of Pacific Networks' peering relationships with other U.S. providers at the Points of Presence (PoP) located in the United States.

Pacific Networks does not have any peering relationships with U.S. providers for the exchange of Internet traffic, since it only provides MPLS VPN service to its customers and does not peer with other providers for the exchange of Internet traffic, as explained in response to Question 16. As stated in the OSC Response, Pacific Networks maintains various physical

points of interconnection with unaffiliated carriers to provide the international circuits used by its MPLS VPN customers for communication with customer sites located outside the U.S.<sup>118</sup>

19. A detailed response that explains the discrepancies and/or omissions, as described in this Order, concerning: (1) ComNet’s statements to the Senate’s Permanent Subcommittee on Investigations, as described in the PSI Report, and the statements made by Pacific Networks and ComNet in response to the Order to Show Cause; and (2) if statements made to the Commission were not accurate and complete when filed, provide accurate and complete responses to explain the discrepancies and/or omissions and to ensure the Commission has all relevant information to conduct its assessment.

The *Order* alleges that there were discrepancies in information to the Senate Subcommittee in two main areas: the location of U.S. records and the involvement of ComNet’s indirect owners in its day-to-day management.

#### Location of Records

The *Order* states that

ComNet representatives informed the Senate Subcommittee that “its data center and all backed-up information are located in the United States and that it controls access to all U.S. records and data systems.” ComNet also informed the Senate Subcommittee that “its parent companies do not have direct access to these records and that they would need to request access from ComNet and follow ComNet’s local procedures.”<sup>119</sup>

The *Order* then characterizes this statement as contradictory to information provided to Team Telecom, stating that

The PSI Report stated that “records of Team Telecom’s site visits indicate that ComNet used [CITIC Tel’s] data center in Hong Kong as a backup and that ComNet’s wholesale billing records ‘are maintained in Hong Kong.’” The PSI Report further stated that “Team Telecom’s records from the 2018 site visit also note that ComNet’s VoIP customer and billing records are accessible to Hong Kong personnel.”<sup>120</sup>

---

<sup>118</sup> *Id.* at 12-13, Exhibits E, G, I.

<sup>119</sup> *Order* at ¶ 56 (footnotes omitted); *see also id.* at ¶ 30.

<sup>120</sup> *Id.* at ¶ 30 (footnotes omitted); *see also id.* at ¶ 56.

The Companies provide a detailed description of the location of U.S. records for Wholesale IDD, Retail Calling Card and MPLS VPN services in response to Question 6. This information is entirely consistent with the information provided to Team Telecom during various site visits and follow ups.

During ComNet's exchanges with Senate Subcommittee staff on April 13, 2020 and afterwards, ComNet representatives understood questions about the location of databases and customer records to refer only to records involved in the provision of VoIP service. As stated in response to Question 6, above, originals, backups and copies of those records related to VoIP service are stored only in the U.S., the Companies' parent companies do not have direct access to this data, and any access by anyone outside the U.S. would need to follow the standard process managed by ComNet for authorizing access to the data. The Companies did not understand the Senate Subcommittee to ask about the location of databases or records related to Wholesale IDD, Retail Calling Card or MPLS VPN services.

It is not surprising that multiple interviews with multiple different U.S. government entities regarding technical matters related to multiple different common carrier and non-common carrier services might result in superficially inconsistent information, warranting subsequent clarification before jumping to the conclusion that the Companies intended to provide inconsistent information. The Companies had no such intent, and, indeed, it would be exceedingly foolish for the Companies to do so, given the volume of information voluntarily and consistently disclosed to Team Telecom since 2009 and subsequently disclosed to the Commission in the OSC Response, not to mention the consequences of providing inconsistent information.

### Involvement in Day-to-Day Management

The alleged discrepancies related to management are statements related to (i) involvement in daily operations, (ii) guidance of information security policies and (iii) monitoring provided by CITIC Tel’s Hong Kong Service Operations Center (“SOC”), referred to as a “NOC” in the PSI Report.

While these discrepancies are addressed below, the Companies first address whether any of the information provided to the Senate Subcommittee constitutes any kind of material omission in providing information in the OSC Response. The Companies categorically deny that omitting any such information was their intent. Relevant to the question of control, the *OSC* asked specific questions regarding current ownership and control, corporate governance, and individuals serving as officers, directors and senior management of the Companies and their upstream ownership.<sup>121</sup> The *OSC* also asked numerous very specific questions about the Companies’ services, equipment and interconnection agreements.<sup>122</sup> The Companies provided hundreds of pages of interconnection agreements, technical diagrams and other documents in response. The *OSC* did not, however, similarly ask the Companies for information regarding location of databases or intercorporate arrangements, as was raised and discussed in the briefing with Senate Subcommittee staff. The Companies reasonably believed information responsive to the Commission would focus on the extent to which executives of the indirect owners played a role in controlling the activities of the Companies, not on whether the Companies received any services whatsoever from affiliates. Thus, the Companies’ statements in the OSC Response

---

<sup>121</sup> *OSC* at ¶ 9.

<sup>122</sup> *Id.*

focused on the limited nature of involvement by indirect owners and their executives. Even so, the Companies provided the CITIC Tel Information Security Policy (and numerous other documents) as part of their response though they were not specifically asked to do so. Certainly, had the Commission made clear that it considered any interaction at all between the Companies and their affiliates to be relevant (much less material) to the question of “control” over operations by adding one more question to its list of specific governance or operational questions, or asked for clarification of information in the OSC Response as compared to information provided to the Senate Subcommittee or at any time in the almost 10 months between release of the PSI Report and release of the *Order*, the Companies would have provided it.

The Companies thus provide the following additional information, as explained further in this response. Nevertheless, the Companies reject the Commission’s contention that because certain issues described in further detail below were discussed with Senate Subcommittee staff the Companies had any intent to withhold this information from the Commission.

Related to daily operations, the *Order* states:

The PSI Report stated that ComNet representatives informed the Senate Subcommittee “that its daily operations are managed by its local management team in California. The representatives, however, acknowledged that [CITIC Tel] reviews the company’s budget and U.S. locations.”<sup>123</sup>

The statement that CITIC Tel “reviews the company’s budget” is based on a statement to the Senate Subcommittee staff that ComNet discusses its budget with CITIC Tel to ensure that the parent company is advised and to address any questions CITIC Tel may have regarding

---

<sup>123</sup> *Order* at ¶ 26 (footnotes omitted).

budget items. This statement does not contradict the statements in the OSC Response related to involvement of ComNet’s indirect owners in financial matters.<sup>124</sup>

The statement that CITIC Tel “reviews the company’s . . . U.S. locations” does not accurately reflect CITIC Tel’s limited involvement. ComNet representatives explained to the Senate Subcommittee staff that specific decisions as to the location of the ComNet’s operations in the U.S. are made by local management, and that any re-location would be reported to CITIC Tel. Again, this statement does not contradict the statements in the OSC Response regarding CITIC Tel’s limited involvement in the ComNet’s day-to-day operations.

Related to guidance on information security policies, the *Order* states:

Significantly, the PSI Report stated that “[CITIC Tel] also guides ComNet on its information security policies,” and that “ComNet maintains a company specific policy, but that policy was drafted based on [CITIC Tel’s] guidance.”<sup>125</sup>

This information is not by any means new. As noted above in response to Question 2 and as required by the 2009 Letter of Assurance, ComNet provided Team Telecom with the Pacific Networks Corp. IT Security Policy, which was adapted from the then current CITIC Tel policy. A copy is provided at Exhibit F to facilitate comparison to the later CITIC Tel policies. As the *Order* recounts, ComNet then advised Team Telecom in 2017 that

[REDACTED]

---

<sup>124</sup> See OSC Response at 11 (“The financial positions of Pacific Networks and ComNet are routinely reviewed by CITIC Tel . . .”), 25 (“Non-American owners of the Companies may routinely review the financial positions of the U.S. based companies, in a similar fashion to how any investor might track an investment in another entity.”) and Declaration (“The extent of involvement of executives of the parent corporations of Pacific Networks and ComNet is to routinely review the financial positions of Pacific Networks and ComNet. These reviews relate only to revenues from and costs of operations, and do not impose any specific obligations with regard to technical or commercial operations.”).

<sup>125</sup> *Order* at ¶¶ 26, 55 (footnotes omitted).



[REDACTED]

As shown by Exhibit K to the OSC Response, the Companies provided the Commission not only with this Team Telecom communication but with all of the documents attached to the correspondence.

The guidance provided to the Companies by the CITIC Tel Information Security Policy has thus been a part of the ComNet’s information security approach since Pacific Networks acquired ComNet. And this should not be surprising: any corporate entity with multiple affiliates involved in handling communications and information technology would want to avoid the inefficiencies and increased chance of compromise created by using different policies.

Importantly, the policy relates to a single aspect of ComNet’s operations: handling of data security. Obviously, and particularly in the context of this inquiry, this is an important matter. But the promulgation of consistent data security policies across affiliated entities does not somehow change ComNet from having independence in its day-to-day operations to having all of its decisions dictated by indirect owners, as the *Order* implies. Moreover, the CITIC Tel Information Security Policy and associated documents are by no means extraordinary policies for managing IT systems. As detailed in response to Question 9, these policies provide the kind of protections and processes that one would expect to apply to any telecommunications or information service provider, and do so in a way that allows local management flexibility in implementation. [REDACTED]

---

<sup>126</sup> *Id.* at ¶ 27 (footnotes omitted).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

As noted by the *Order*, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Having provided the IT policy to the U.S. government as far back as 2009, and included the then-current policy in the OSC Response, it is not accurate to characterize the existence of the policy as a discrepancy with the PSI Report or an intentional omission of information, much less a failure of candor and transparency. The Companies acknowledge, however, that in stating that the Companies’ indirect owners “do not assess or require changes in the Companies’ technical or network operations” and “do not impose any specific obligations with regard to technical or commercial operations”<sup>129</sup> the Companies should have clarified that while the

---

<sup>127</sup> *Id.* n.128.

<sup>128</sup> *Id.* at ¶ 27.

<sup>129</sup> OSC Response at 11, Declaration.

Companies’ indirect owners may not require that specific technical decisions be made on a day-to-day basis, the Companies observe guidance from CITIC Tel regarding network security. Given that, again, this information has been repeatedly disclosed to the U.S. government, it would be manifestly unfair to characterize this as an intentional failure to respond to the Commission with transparency on this matter.

Related to monitoring, the *Order* states:

[T]he PSI Report stated that “ComNet leverages [CITIC Tel’s] network operations center [(NOC)], located in Hong Kong, for ‘first tier monitoring’ against cyber incidents or disruptions. “All system alarms and network management data are sent to the NOC . . . .” Further, [CITIC Tel’s] NOC maintains records of all alarms and access logs generated by ComNet’s systems.”<sup>130</sup>

The cybersecurity monitoring and protective service provided to ComNet by the Hong Kong SOC (as described above in response to Questions 9 and 15) is the same kind of service provided to telecommunications and information service providers by affiliated and third party vendors around the world. Further, it should not come as a surprise that a subsidiary of a corporation with an advanced network operations center would choose to use that facility rather than develop its own redundant facilities. None of the other numerous providers using externally provided threat monitoring would consider that outsourcing incident monitoring would in any way compromise their independent operation, and neither does ComNet: in the event of any incident ComNet’s local engineers are still responsible for taking whatever actions are necessary to protect its services and customers. ComNet provided this information to the Senate Subcommittee staff as a specific response to a discussion regarding network support and threat monitoring. ComNet did not consider this particular fact to show “control” by CITIC Tel or

---

<sup>130</sup> *Order* at ¶¶ 26, 50 and 55 (footnotes omitted).

other indirect owners. As such, any failure to provide this information to the Commission was not intentional and ComNet could have clarified if asked following release of the PSI Report.

Although not a discrepancy between the PSI Report and the OSC Response, the *Order* states:

Pacific Networks and ComNet certify “under penalty of perjury” that . . . “[e]xecutives of [the Companies’] parent corporations do not participate in the daily operations of ComNet or Pacific Networks.” However, Exhibits B and C of their response shows that the two directors of Pacific Networks and ComNet are also Executive Directors of CITIC Tel. One of these individuals is Chief Executive Officer of CITIC Tel, while the other individual is the Chief Financial Officer of CITIC Tel. In addition to CITIC Tel, the two directors of Pacific Networks and ComNet are also directors of Pacific Choice International Limited. These two individuals are the only persons identified in Pacific Networks’ and Pacific Choice International Limited’s corporate leadership. Pacific Networks and ComNet further state that “[n]o other officers or senior officials are employed by Pacific Networks Corp.” and “[n]o other officers or senior officials are employed by Pacific Choice International Limited.” Pacific Networks’ and ComNet’s statements are inconsistent . . . .<sup>131</sup>

These statements are in no way inconsistent. The OSC Response stated that executives of the Companies’ parent corporations do not participate in their daily operations. As stated in response to Question 2, above, neither Mr. Cai Da Wei nor Mr. Li Bing Chi, Esmond, the directors of the Companies, spend any significant time controlling the Companies’ affairs, much less involving themselves in the Companies’ day-to-day management, given that they are only required to make financial decisions for the Companies as described above.

In sum, in its effort to find as many inconsistencies as possible to support revocation of the Companies’ Section 214 authorizations, the Commission ignores important distinctions and conflates consultation and guidance with day-to-day control.

---

<sup>131</sup> *Id.* at ¶ 59 (footnotes omitted).

Finally, given the Order's focus on intercorporate arrangements, and to ensure the Commission is advised of the relationships between the Companies and affiliates in Hong Kong, they provide this additional information regarding Pacific Networks. As stated above in response to Question 6, individuals employed by [REDACTED] a subsidiary of CITIC Telecom, have access to U.S. customer records to provide support and billing. As stated in response to Question 15, [REDACTED] provides first tier support for Pacific Networks' MPLS VPN service. Both of these services are provided to Pacific Networks pursuant to a services contract with [REDACTED] [REDACTED] a subsidiary of [REDACTED] a copy of which is attached hereto as Exhibit J.<sup>132</sup> Other support services provided under this contract are [REDACTED]

██████████ The contract states that Pacific Networks has the authority to oversee and direct the

<sup>132</sup> Neither of these subsidiaries is a direct or indirect owner of either of the Companies. They are thus affiliates, not owners, of Pacific Networks.

day-to-day operations of its business, and that all services under the contract are provided at Pacific Networks' direction. Specifically, the contract makes clear that it is not intended to limit and does not limit Pacific Networks' (i) full access to its equipment and facilities, (ii) control over its daily operations, (iii) control over its telecommunications network, (iv) control over its policy decisions including the preparation and filing of applications and reports with the Commission and other agencies, (v) control over the employment, supervision and dismissal of Pacific Networks employees, (vi) responsibility for payment of financial obligations, and (vii) receipt of money for provision of services.

20. An identification of the percentage of calls using IDD service that use SS7 compared to SIP based Interconnected VoIP.

In 2020, the total percentage of SS7 traffic as compared to SIP based Interconnected VoIP was less than [REDACTED] % of ComNet's total Wholesale IDD service traffic.

21. An identification of the percentage of A2P messages that are sent through IP based networks versus SS7.

In 2020, [REDACTED] % of A2P SMS connections used IP based networks.

22. A detailed description of the measures to ensure privacy and integrity of data stored in ComNet's facilities supporting current and near future section 214 authority services.

Please see the answer to Question 9 providing details as to measures taken by ComNet to ensure the privacy and integrity of data stored in ComNet's facilities supporting current and near future Section 214 authority service. Please also see answers to Questions 6, 7 and 12 regarding policies and measures taken to restrict access to data and protect privacy.

23. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

24. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

25. Copies of the letters sent to the Commission confirming implementation of both ISPCs (3-193-4 and 3-191-6).

The International Bureau granted ComNet's applications for ISPCs in 2001 and 2003,<sup>133</sup> under ComNet's prior ownership. ComNet cannot now locate copies of letters to the Commission confirming implementation of the ISPCs, nor do the letters appear in the relevant files in the International Bureau Filing System.

The Commission should not, however, use the absence of such a letter as a reason to reclaim ComNet's ISPCs. The standard letter issued to recipients of ISPCs states that "[u]nless this office is specifically notified of the actual implementation of assignments for planned future service, it will be assumed that those implementations did not occur and such assignments will expire, making those codes available for reassignment."<sup>134</sup> The Commission has not, however, adopted regulations specifying that reclamation of ISPCs is mandatory in the event of a failure to

---

<sup>133</sup> See File Nos. SPC-NEW-20010528-00019 (ISPC 3-191-6); SPC-NEW-20030529-00021 (ISPC 3-193-4).

<sup>134</sup> See Letter from Cathy Hsu, FCC, to Rob Leon, Senior Technical Manager, CM Tel (USA) LLC, File No. SPC-NEW-20030529-00021 (Jun. 13, 2003). A copy of this letter was helpfully uploaded to IBFS, presumably by International Bureau staff, on February 12, 2021. The file for ISPC 3-191-6 does not have a record of the grant letter for that code.



file an implementation notification, and any assumption that the implementation did not occur is contradicted by ComNet's actual implementation and continued use of the ISPCs. While the International Bureau recently reclaimed ISPCs from both China Telecom and China Unicom, in both cases the International Bureau concluded that the ISPCs were not in use and that retention for future use was not sufficient to allow the companies to continue to retain their ISPC assignments.<sup>135</sup> Without otherwise opining on the validity of the reclamations in those cases, the Companies submit that because of ComNet's ongoing use of the ISPCs, their case is in an entirely different posture.

26. An explanation as to whether both ISPCs (3-193-4 and 3-191-6) have been in continuous use since their implementation.

ComNet confirms that both ISPCs have been in continuous use since their implementation. When Pacific Networks acquired ComNet in 2009, ComNet's voice network only used TDM, and thus used both ISPCs. A decline in use of the ISPCs only began to occur later, as more traffic moved to IP networks. ComNet, however, does continue to use both ISPCs.

27. An explanation of why ComNet needs two ISPCs for the [REDACTED]

Although the volume is low, ComNet uses two ISPCs to interconnect [REDACTED] through a redundant pathway, in order to provide resiliency and avoid a single point of failure.

---

<sup>135</sup> See Letter from Denise Coca, Chief, Telecommunications and Analysis Division, International Bureau, FCC, to Robert E. Stup, Jr. and Paul C. Besozzi, Counsel for China Unicom (Americas) Operations Limited, DA 21-227 (Mar. 10, 2021); Letter from Denise Coca, Chief, Telecommunications and Analysis Division, International Bureau, FCC, to Zhao-feng Ye and Xiaoyi Liu, China Telecom (Americas) Corporation, DA 20-1369 (Nov. 18, 2021).

Accordingly, as long as ComNet continues to provide interconnection to [REDACTED] it considers the use of both ISPCs as necessary for prudent network management.

28. An explanation concerning whether the Traffic and Revenue reports submitted for the years 2003-2014 reflected use of one or both of these ISPCs.

The Companies can confirm that the Traffic and Revenue reports submitted from 2008-2014 reflect the use of both ISPCs. Traffic and Revenue reports for 2003-2007 were submitted by ComNet's prior owner, and the Companies cannot now locate the reports to confirm what may have been reflected in them. The Companies assume, however, that these earlier reports would reflect use of the same two ISPCs as reflected in the 2008-2014 reports.

29. An explanation as to why Traffic and Revenue reports were not submitted for the years 2003, 2005, and 2007.

Pacific Networks completed its acquisition of ComNet in 2009. The Companies are not aware of the reason why ComNet's prior owner did not submit Traffic and Revenue reports in 2003, 2005 and 2007.

30. An explanation as to whether Pacific Networks and ComNet filed with the Commission corrected versions of the pro forma transfer of control notifications originally filed with the Commission on January 26, 2012, that they provided to DHS and DOJ on February 16, 2012; and if corrected versions of the pro forma transfer of control notifications were not filed with the Commission, Pacific Networks and ComNet shall file the corrected pro forma notifications in IBFS.

Counsel for Pacific Networks and ComNet emailed corrected version of the pro forma transfer of control notifications to Commission staff on February 16, 2012. The cover email showing the attached notifications is attached hereto as Exhibit G, together with the corrected notifications as sent to the Commission. The Companies shall file copies of these corrected notifications in IBFS after filing this response.

31. A complete description of all work required for Pacific Networks and ComNet to discontinue all section 214 services to their customers if the Commission were to revoke

and/or terminate Pacific Networks' and ComNet's section 214 authorities, along with a detailed estimate of the time required for each portion of that work and an explanation of how that estimate was reached.

#### ComNet's Calling Card Service

Based on ComNet's current records, over [REDACTED] calling cards have been issued, but not yet been used for the first time. The use of each card is time limited in two ways. First, following the first use of the card, the card will expire at the end of a term printed on the back of the card. This term can range from [REDACTED] days after its first date of use. Second, under ComNet's standard terms and conditions, an unused calling cards will expire in [REDACTED] years. With a monthly average of [REDACTED] cards being newly activated with first use, ComNet estimates that it may take as many as [REDACTED] months from any given date for all unused cards issued as of that date to be used or expire.

Most of the calling cards are being sold via ComNet's wholesale agents and retail store agents. For interruption or termination of card delivery, ComNet must provide advance notification to both wholesale agents and retail store agents. Wholesale agents distribute ComNet's calling cards to smaller agents and out-of-town stores, and it may take them at least 3 to 6 months to coordinate and collect all the unsold cards from each of the stores in different cities/regions. Retail store agents sell ComNet's calling cards direct to customers, and would handle all returned card and refund requests from customers. Some of the retail stores may be temporarily closed due to COVID-19 restrictions, and this may cause further delay in recalling unused cards.

ComNet has had over [REDACTED] unique callers use its calling card service in the last 12 months. To honor the expiry term for the cards that have already been sold to customers, ComNet would need to continue to provide service. In this regard, it will be more difficult for

ComNet's customers to find replacement services than it would be for average customers, given that many of ComNet's customers prefer Mandarin, Cantonese or other foreign-language customer support and would need to find an alternative provider that offers such support.

Accordingly, in order to ensure that ComNet's Calling Card customers have an opportunity to use the service they have already purchased, honor ComNet's service obligations and expiry terms and minimize disruption to ComNet's customers, ComNet would need at least 24 months to terminate Retail Calling Card service in the United States.

#### ComNet's Wholesale IDD Service

ComNet serves [REDACTED] customers through its [REDACTED] gateway (the Wholesale IDD platform) in the Los Angeles data center.<sup>136</sup> To discontinue the Wholesale IDD service in the U.S. provided by ComNet, CITIC Tel would need to sign service contracts directly with the Wholesale IDD customers for access to its voice gateway in Hong Kong if they wish to continue to have such access. Note that CITIC Tel would not itself provide international service into or out of the U.S.—CITIC Tel would provide a voice gateway in Hong Kong, but customers would no longer use ComNet's [REDACTED] gateway in Los Angeles, and would need to establish new VoIP SIP/TDM connections to reach CITIC Tel's Hong Kong gateway.

The time required for the above steps is as follows.

- ComNet estimates 3-4 months to notify customers and move contracts.

---

<sup>136</sup> In the OSC Response, Exhibit E listed [REDACTED] customers for Wholesale IDD service, [REDACTED] of which are now no longer served by ComNet. A revision to this portion of the OSC Response, Exhibit E, is attached hereto as Exhibit H.

- Once completed, ComNet estimates 1-2 months to establish new connections to the voice gateway in Hong Kong for customers wanting to continue to access the Hong Kong gateway.
- After installation, ComNet estimates approximately 2 weeks to complete voice quality tests on newly established circuits with all [REDACTED] customers and launch new service.

Separate from the migration of ComNet customers, ComNet's Calling Card platform also uses the Wholesale IDD service, with a total of seven active VoIP SIP connections to the [REDACTED] gateway in the Los Angeles data center. ComNet would need to continue to maintain those Wholesale IDD links for the 24 months necessary for most calling cards to expire.

Accordingly, ComNet estimates that it would take approximately 6-9 months to migrate third party customers and discontinue Wholesale IDD service, and as long as 24 months to migrate the seven Wholesale IDD connections provided to ComNet's Calling Card service, given the need to maintain the connections to the [REDACTED] gateway.

#### Pacific Networks' MPLS VPN Service

Pacific Networks' existing service orders for MPLS VPN service have a remaining service term of up to [REDACTED] months. The provision of the service typically involves connectivity from customer locations to Pacific Networks' location, and as such the service requires leased lines and the delivery of hardware and/or software specially tailored to meet the customers' particular needs.

Accordingly, termination of Pacific Networks' MPLS VPN service requires Pacific Networks to contact each customer to carry out an assessment of the costs involved based on the customers' particular service needs and the availability of capacity, facilities or other necessary

resources. Pacific Networks will then approach vendors for their proposal of the work and equipment necessary to transition the service, forward vendor proposals for review by customers, and coordinate conclusion of service contracts. Pacific Networks can then work with the vendors to transition the customer connections to a MPLS VPN service provider of the customer's choosing.

Depending on customer need, the availability of vendors in customer areas, and the time required for finalizing the necessary arrangements and contracts acceptable to both customers and vendors/suppliers, Pacific Networks estimates that it will take approximately 12-19 months to complete migration of MPLS VPN services. A breakdown of the time estimate for the above series of steps is as follows:

Step	Description	Estimate of time required
i.	Pacific Networks to send sales representative(s) to approach each of its customers to gauge their need for service.	1-2 months
ii.	Pacific Networks to carry out an assessment of the costs involved, availability of capacity, facilities or other necessary resources, or other business considerations based on customers' needs.	1-2 months
iii.	Pacific Networks to approach vendors/suppliers for their proposal of necessary arrangements, contracts and related terms and conditions and then forward for review by customers.	1-2 months
iv.	Pacific Networks to coordinate between customers and vendors/suppliers for the necessary arrangements, contracts and related terms and conditions.	1-2 months
v.	Pacific Networks to facilitate contracts to be signed by the	1-2 months

	customers and the vendors/suppliers, assist the customers to complete and place service orders to the vendors/suppliers.	
vi.	Pacific Networks to coordinate between the customers and vendors/suppliers the provisioning of the new services, including but not limited to customer site survey, letters of authorization, physical cabling work and user acceptance test.	3-5 months
vii.	Pacific Networks to review and study the latest technical setup of the customer's infrastructure, prepare and propose a cut-over plan to the customer. Pacific Networks and the customer shall discuss and agree on the cut-over plan.	1 month
viii.	Pacific Networks to carry out the cut-over according to the cut-over plan from existing services to new services with the customers and vendors/suppliers.	1 month
ix.	Upon successful cut-over, Pacific Networks to terminate the services with existing suppliers.	2 months
	Total:	12-19 months

32. With reference to ComNet's cloud-based VoIP service, the Commission directed Pacific Networks and ComNet to fully explain the IP service offering or whether this is an interconnected VoIP service offering as defined by the Commission's rules and any security measures concerning this service.

As noted above, the Order directed the Companies to answer this question but did not include it in the Appendix A list, so the Companies have added this question and response.

ComNet's cloud-based VoIP service provides enterprise users the functions of an office telephone system without hosting a physical PBX in the office. It thus provides an IP-based voice functionality to office users, enabling them to make both national and international calls to

numbers on the Public Switched Telecommunications Network through ComNet's wholesale voice switch. Each VoIP phone used with the service is registered using a username and strong password protection on ComNet's VoIP Soft Switch located in ComNet's Los Angeles data center. The Soft Switch validates the specific brands of SIP phones used for the service, in order to avoid unauthorized devices being attached to the network. ComNet takes outgoing calls and routes them only to an outgoing trunk connected to ComNet's wholesale voice switch, then uses SIP trunks to route to the ultimate destination. A diagram showing how the service is provisioned is attached hereto as Exhibit I.<sup>137</sup> Additionally, an updated customer list is provided as Exhibit H.

As the Companies stated in the OSC Response,<sup>138</sup> they consider this service to qualify under the Commission's rules as an interconnected VoIP service that does not require a Section 214 authorization.

With regard to other security measures applicable to the service, as stated in response to Question 6, originals, backups and copies of the VoIP records are only stored in the U.S., access is governed by Section 10 of the CITIC Tel Information Security Policy, and any access to such records by anyone located outside the U.S. must be authorized on an individual basis.

**V. SHOULD THE COMMISSION REVOKE THE COMPANIES' AUTHORIZATIONS, THE COMMISSION MUST PROVIDE A MEANINGFUL TRANSITION PERIOD FOR EXISTING CUSTOMERS**

The Commission must consider measures to protect the interests of the tens of thousands of customers that would be affected if the Commission were to revoke the Companies' Section

---

<sup>137</sup> This diagram updates the diagram for the VoIP service provided as part of the presentation to DoJ in 2018 which appears in Exhibit D at slide 22.

<sup>138</sup> OSC Response at 14.



214 authorizations. Congress recognized the harm that would be incurred by customers from a sudden discontinuance of service and placed restrictions on a carrier's ability to affect such service without prior authorization: Section 214(a) of the Act provides that "[n]o carrier shall discontinue, reduce or impair service to a community, or part of a community, unless and until there shall first have been obtained from the Commission a certificate that neither the present nor future public convenience and necessity will be adversely affected thereby." The Commission should likewise consider the effect a sudden revocation of the Companies' Section 214 authorization would have on the public convenience and necessity. Accordingly, should the Commission decide to revoke the Companies' authorizations, the Companies urge the Commission to provide for a transition period sufficient to allow the termination of the Companies' services without customer disruption as described in response to Question 31.

## VI. CONCLUSION

Despite the Companies' efforts to provide the Commission with responsive information, the *Order* nevertheless excoriates the Companies for a supposed lack of transparency, raising the question of why the Commission is conducting any further fact-finding. Nevertheless, the Companies have again tried to meet the Commission's requests. As the Commission refuses to conduct an evidentiary hearing as is required given the circumstances, if Commission staff has any questions or believes there are any further inconsistencies in the information provided by the Companies, the Companies hope that staff will at least engage with the Companies, ask questions, and provide them an opportunity to explain. This response, together with the materials provided in the OSC Response, demonstrates why the Commission should not revoke the Companies' section 214 authorizations, or reclaim its ISPCs. Certainly, it demonstrates why the Commission should not proceed with the process the *Order* fails to justify.

**Declaration of Li Ying (Linda) Peng**

My name is Li Ying (Linda) Peng, and I am the General Manager, Human Resources and Administration of ComNet (USA) LLC (“ComNet”). I am making this Declaration in support of a Response (“Response”) to an Order Instituting Proceeding on Revocation and Termination released by the Federal Communications Commission regarding ComNet and its parent company, Pacific Networks Corp (“Pacific Networks” and, together with ComNet, the “Companies”). I hereby certify under penalty of perjury that the statements in this Declaration are true and accurate to the best of my knowledge, information and belief.

1. I am a U.S. citizen resident in the State of California, and, since 2013, have served as the managing officer for the Companies in the United States. I am the point of contact for accepting and overseeing compliance with wiretap orders, pen/trap orders, subpoenas and other lawful demands by U.S. law enforcement authorities, and other lawful demands by U.S. law enforcement for the content of communications and any records relating to communications services offered by the Companies to U.S. persons.
2. At no time have any officials of the government of the People’s Republic of China or of the Chinese Communist Party directed or requested that Pacific Networks or ComNet take or refrain from taking any particular action.
3. Under the terms of the Companies’ 2009 Letter of Assurance on file with the Federal Communications Commission, the Companies provided the interagency committee led by the Department of Justice and Department of Homeland Security known as “Team Telecom” with a copy of the Pacific Networks Corp. IT Security Policy, which was derived from the then current Information Security Policy of CITIC Telecom International Holdings Limited (“CITIC Tel”). The Companies’ counsel advised Team Telecom in 2017 when that policy was succeeded by the CITIC Tel Information Security Policy, which was provided to Team Telecom at that time.
4. The Companies have at all times complied with law enforcement requests and Team Telecom requests.
5. The statements of fact disclosed by the Companies in the Response, including statements regarding the Companies’ management, control and operations in response to Questions 1 through 32 at Section IV of the Response, are true and correct to the best of my knowledge, information and belief.

/s/ Li Ying Peng  
Li Ying (Linda) Peng

April 28, 2021

**EXHIBIT A**

**Articles of Incorporation and Bylaws for Pacific Networks Corp.  
ComNet (USA) LLC Limited Liability Company Agreement**

# Delaware

PAGE 1

*The First State*

I, HARRIET SMITH WINDSOR, SECRETARY OF STATE OF THE STATE OF DELAWARE, DO HEREBY CERTIFY THE ATTACHED IS A TRUE AND CORRECT COPY OF THE CERTIFICATE OF INCORPORATION OF "PACIFIC NETWORKS CORP.", FILED IN THIS OFFICE ON THE FIFTEENTH DAY OF JUNE, A.D. 2007, AT 1:34 O'CLOCK P.M.

A FILED COPY OF THIS CERTIFICATE HAS BEEN FORWARDED TO THE KENT COUNTY RECORDER OF DEEDS.

4362760 8100

070715129



*Harriet Smith Windsor*

Harriet Smith Windsor, Secretary of State

AUTHENTICATION: 5763780

DATE: 06-15-07

State of Delaware  
 Secretary of State  
 Division of Corporations  
 Delivered 01:43 PM 06/15/2007  
 FILED 01:34 PM 06/15/2007  
 SRV 070715129 - 4362760 FILE

**CERTIFICATE OF INCORPORATION**  
**OF**  
**PACIFIC NETWORKS CORP.**

**FIRST:** The name of the corporation is Pacific Networks Corp. (the "Corporation").

**SECOND:** The name and address of the Corporation's registered office in the State of Delaware are National Corporate Research, Ltd., 615 South DuPont Highway, Dover, Delaware 19901, Kent County.

**THIRD:** The purpose of the Corporation is to engage in any lawful act or activity for which corporations may be organized under the General Corporation Law of Delaware.

**FOURTH:** The Corporation is authorized to issue one class of shares to be designated "Common Stock." The number of shares of Common Stock authorized to be issued is One Million (1,000,000) with a par value of \$0.00001 per share.

**FIFTH:** In furtherance and not in limitation of the powers conferred by statute, the Board of Directors is expressly authorized to make, alter, amend or repeal the bylaws of the Corporation.

**SIXTH:** Meetings of the stockholders of the Corporation may be held within or without the State of Delaware, as the bylaws may provide. The books of the Corporation may be kept (subject to any provision contained in the statutes) outside the State of Delaware at such a place or places as may be designated from time to time by the Board or in the bylaws of the Corporation.

**SEVENTH:** The election of directors need not be by written ballot unless a stockholder demands election by written ballot at the meeting and before the voting begins or unless the bylaws of the Corporation so provide. At all elections of directors of the Corporation, each holder of stock of any class or classes or of any one or more series thereof shall be entitled to as many votes as shall equal the number of votes which (except for this provision as to cumulative voting) he would be entitled to cast for the election of directors with respect to his shares of stock multiplied by the number of directors to be elected by him, and he may cast all of such votes for a single director or may distribute them among the number to be voted for, or for any two or more of them as he may see fit.

**EIGHTH:** To the fullest extent permitted by the Delaware General Corporation Law, and to the extent applicable, to the fullest extent permissible under California law, both as the same exists or as may hereafter be amended, a director of the Corporation shall not be personally liable to the Corporation or its stockholders for monetary damages or breach of fiduciary duty as a director. The Corporation shall indemnify to the fullest extent permitted by law any person made or threatened to be made a party to an action or proceeding, whether criminal, civil, administrative, or investigative, by reason of the fact that he or she, his or her

PAL0AL.T0/105117.1

testator or intestate is or was a director or officer of the Corporation or any predecessor of the Corporation, or serves or served at any other enterprise as director or officer at the request of the Corporation or any predecessor to the Corporation. Neither any amendment nor repeal of this Article, nor the adoption of any provision of this Certificate of Incorporation inconsistent with this Article, shall eliminate or reduce the effect of this Article in respect of any matter occurring, or any cause of action, suit or claim that, but for this Article would accrue or arise, prior to such amendment, repeal or adoption of an inconsistent provision.

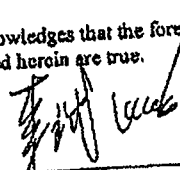
NINTH: The duration of the Corporation shall be perpetual.

TENTH: The Corporation shall not be subject to or governed by the provisions of Section 203 of the Delaware General Corporation Law, or any amendment or successor provisions thereto, with respect to business combinations between the Corporation and interested stockholders.

ELEVENTH: The Corporation reserves the right at any time, and from time to time, to amend, alter, change or repeal any provision contained in this Certificate of Incorporation, and other provisions authorized by the laws of the State of Delaware at the time in force may be added or inserted, in the manner now or hereafter prescribed by law; and all rights, preferences and privileges of whatsoever nature conferred upon stockholders, directors or any other persons whomsoever by and pursuant to this Certificate of Incorporation in its present form or as hereafter amended are granted subject to the rights reserved in this Article.

TWELFTH: The name and mailing address of the incorporator are as follows:  
Bin Li, Flat A, 37<sup>th</sup> Floor, Block 1, Harbourfront Landmark, 11 Wan Hoi Street, Hunghom,  
Kowloon, Hong Kong.

The undersigned incorporator hereby acknowledges that the foregoing Certificate of Incorporation is his act and deed and that the facts stated herein are true.



Dated: June 15, 2007

Bin Li, Incorporator

---

**BYLAWS  
OF  
PACIFIC NETWORKS CORP.**

---

**A DELAWARE CORPORATION**

PALOALTO/105131.2

**PAGES A-6 THROUGH A-26 REDACTED AS  
CONFIDENTIAL**



## State of Delaware

Office of the Secretary of State

I, EDWARD J. FREEL, SECRETARY OF STATE OF THE STATE OF DELAWARE, DO HEREBY CERTIFY "CM TEL (USA) LLC" IS DULY FORMED UNDER THE LAWS OF THE STATE OF DELAWARE AND IS IN GOOD STANDING AND HAS A LEGAL EXISTENCE SO FAR AS THE RECORDS OF THIS OFFICE SHOW, AS OF THE NINETEENTH DAY OF JULY, A.D. 1999.

AND I DO HEREBY FURTHER CERTIFY THAT THE ANNUAL TAXES HAVE NOT BEEN ASSESSED TO DATE.

AND I DO HEREBY FURTHER CERTIFY THAT THE AFORESAID LIMITED LIABILITY COMPANY IS DULY FORMED UNDER THE LAWS OF THE STATE OF DELAWARE AND IS IN GOOD STANDING AND HAS A LEGAL EXISTENCE NOT HAVING BEEN CANCELLED OR DISSOLVED SO FAR AS THE RECORDS OF THIS OFFICE SHOW AND IS DULY AUTHORIZED TO TRANSACT BUSINESS.

AND I DO HEREBY FURTHER CERTIFY THAT THE SAID "CM TEL (USA) LLC" WAS FORMED ON THE THIRTEENTH DAY OF JULY, A.D. 1999.

AND I DO HEREBY FURTHER CERTIFY THAT THE EFFECTIVE DATE OF THE AFORESAID IS THE NINETEENTH DAY OF JULY, A.D. 1999.



A handwritten signature in cursive script, reading "Edward J. Freel".

Edward J. Freel, Secretary of State

3068709 8300

991294968

AUTHENTICATION:

9871615

DATE:

07-19-99

199920510003

**PAGES A-28 THROUGH A-51 REDACTED AS  
CONFIDENTIAL**

**EXHIBIT B**

**CITIC Tel Information Security Policy**

**REDACTED – FOR PUBLIC INSPECTION**

**ATTACHMENT REDACTED IN ITS ENTIRETY AS  
CONFIDENTIAL**

**EXHIBIT C**

**Privacy Policies**

February 10, 2021

BY ELECTRONIC FILING  
Marlene H. Dortch Office of the Secretary  
Federal Communications Commission  
445 12th Street, SW Suite TW-A325  
Washington, DC 20554

Re: ComNet (USA) LLC Annual Customer Proprietary Network Information Certification for 2020;  
EB Docket No. 06-36

Dear Ms. Dortch:

Enclosed for filing in the above-referenced docket, please find the 2020 Annual 47 C.F.R. §64.2009(e) Customer Proprietary Network Information Certification for ComNet (USA) LLC ("ComNet"), and an accompanying statement regarding ComNet's operating procedures.

Please do not hesitate to contact me should you have any questions.

Sincerely,

ComNet (USA) LLC



Linda Peng

Enclosures

cc: FCC Enforcement Bureau, Telecommunications Consumers Division  
445 12th Street, SW, Washington, DC 20554  
Best Copy and Printing, Inc. (via email [fcc@bcpiweb.com](mailto:fcc@bcpiweb.com))

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification****EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2021 covering the prior calendar year 2020

1. Date filed: Feb 10, 2021
2. Name of company covered by this certification: ComNet (USA) LLC
3. Form 499 Filer ID: 823684
4. Name of signatory: Linda Peng
5. Title of signatory: General Manager, HRA & Admin
6. Certification:

I, Linda Peng, certify that I am the General Manager of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed:  \_\_\_\_\_

Name: Linda Peng

Title: General Manager

## **CPNI STATEMENT**

The following provisions set forth the ComNet (USA) LLC ("ComNet") operating procedures that ensure it is in compliance with the Commission's customer proprietary network information ("CPNI") rules.

### **Compliance with Federal CPNI Requirements**

#### **1. Definition**

Customer proprietary network information refers to information regarding the quantity, technical configuration, type, destination, and amount of use of service subscribed to by any customer of ComNet, and that is made available to ComNet by the customer solely by virtue of the customer's relationship to ComNet. It also includes information contained in customer bills, if applicable. CPNI does not include subscriber list information.

#### **2. Marketing**

- a) ComNet may use, disclose, or permit access to a customer's CPNI, without customer approval, for the purpose of providing or marketing services to the customer that the customer already utilizes from ComNet.
  - o For customers that subscribe to more than one category of service offered by ComNet, ComNet may share CPNI among its affiliated entities that provide a service offering to the customer.
  - o For customers that do not subscribe to more than one category of service offered by ComNet, ComNet may not share CPNI with its affiliates, except as provided in subsection c).
- b) ComNet shall not use, disclose, or permit access to a customer's CPNI, without customer approval, for the purpose of marketing services to the customer that the customer does not already utilize from ComNet.
  - o ComNet shall not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers.
- c) ComNet may use, disclose, or permit access to CPNI, without customer approval in the following situations:
  - o In ComNet's provision of inside wiring installation, maintenance, and repair services, if any.
  - o For the purpose of conducting research on the health effects of commercial mobile radio services, if any.



## **CPNI STATEMENT**

The following provisions set forth the ComNet (USA) LLC ("ComNet") operating procedures that ensure it is in compliance with the Commission's customer proprietary network information ("CPNI") rules.

### **Compliance with Federal CPNI Requirements**

#### **1. Definition**

Customer proprietary network information refers to information regarding the quantity, technical configuration, type, destination, and amount of use of service subscribed to by any customer of ComNet, and that is made available to ComNet by the customer solely by virtue of the customer's relationship to ComNet. It also includes information contained in customer bills, if applicable. CPNI does not include subscriber list information.

#### **2. Marketing**

- a) ComNet may use, disclose, or permit access to a customer's CPNI, without customer approval, for the purpose of providing or marketing services to the customer that the customer already utilizes from ComNet.
  - o For customers that subscribe to more than one category of service offered by ComNet, ComNet may share CPNI among its affiliated entities that provide a service offering to the customer.
  - o For customers that do not subscribe to more than one category of service offered by ComNet, ComNet may not share CPNI with its affiliates, except as provided in subsection c).
- b) ComNet shall not use, disclose, or permit access to a customer's CPNI, without customer approval, for the purpose of marketing services to the customer that the customer does not already utilize from ComNet.
  - o ComNet shall not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers.
- c) ComNet may use, disclose, or permit access to CPNI, without customer approval in the following situations:
  - o In ComNet's provision of inside wiring installation, maintenance, and repair services, if any.
  - o For the purpose of conducting research on the health effects of commercial mobile radio services, if any.

- o For the purpose of marketing services such as speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.
- d) ComNet may use, disclose, or permit access to CPNI for the purpose of protecting ComNet's rights or property.
- e) ComNet may use, disclose, or permit access to CPNI for the purpose of protecting users of its services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

### **3. Approval Requirements**

- a) Customer approval may be granted orally, electronically, or in writing.
- b) A customer's approval or disapproval shall remain in effect until the customer revokes or limits such approval or disapproval.
- c) In cases where customer approval is required, ComNet shall request approval through either an opt-in or opt-out method.
- d) Opt-in approval requires ComNet to obtain affirmative, express consent from the customer, allowing the requested CPNI usage, disclosure, or access. ComNet shall provide appropriate notification of its request, as explained in section 5 below, to the customer prior to seeking such consent.
- e) Under the opt-out approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object within 30 days of receiving appropriate notification from ComNet of its request, as explained in section 6 below.

### **4. Notice Requirements**

- a) Before requesting customer approval of CPNI usage, ComNet shall provide individual notification to the customer of the customer's right to restrict use of, disclosure of, and access to the customer's CPNI.
- b) The notification shall provide sufficient information to enable the customer to make an informed decision as to whether to permit use, disclosure, or access to the customer's CPNI.
  - o The notification shall state that the customer has a right, and ComNet has a duty, under federal law, to protect the confidentiality of CPNI.
  - o The notification shall specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will

be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

- The notification shall advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and shall clearly state that a denial of approval will not affect the provision of any such services that the customer purchases. ComNet, however, may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.
  - The notification shall be comprehensible and shall not be misleading.
  - If written notification is provided, the notice shall be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to the customer.
  - If any portion of a notification is translated into another language, then all portions of the notification shall be translated into that language.
  - ComNet may state in the notification that the customer's approval to use CPNI may enhance ComNet's ability to offer products and services tailored to the customer's needs. ComNet also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.
  - ComNet shall not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.
  - The notification shall state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from ComNet is valid until the customer affirmatively revokes or limits such approval or denial.
- c) ComNet shall maintain all records of notification for at least one year.

## **5. Opt-in Notice Requirements**

- a) ComNet shall provide notification to obtain opt-in approval through oral, written, or electronic methods.
- b) The contents of an opt-in notice shall comply with the requirements of section 4, subsection b), above.

## **6. Opt-out Notice Requirements**

- a) ComNet shall provide notification to obtain opt-out approval only through written or electronic methods.
- b) The contents of an opt-out notice shall comply with the requirements of section 4, subsection b), above.

- c) ComNet shall wait at least 30 days after providing notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI.
- d) ComNet shall notify customers as to the applicable waiting period for a response before approval is assumed.
  - o In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent.
  - o In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.
- e) For those customers for which ComNet uses an opt-out method, ComNet shall provide notices every two years.
- f) For electronic notifications, ComNet shall comply with the following requirements:
  - o ComNet shall obtain express, verifiable, prior approval from consumers to send notices via email regarding services in general or CPNI in particular;
  - o ComNet shall allow customers to reply directly to emails containing CPNI notice in order to opt-out;
  - o Opt-out email notices that are returned to ComNet as undeliverable shall be sent to the customer in another form before ComNet may consider the customer to have received notice;
  - o ComNet shall ensure that the subject line of the message clearly and accurately identifies the subject matter of the email; and
  - o ComNet shall make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week.

#### **7. Notice Requirements Specific to One-Time Use of CPNI**

- a) ComNet may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether it uses opt-out or opt-in approval, based on the nature of the contract.
- b) The contents of an opt-out notice shall comply with the requirements of section 4, subsection b), above, except that ComNet may omit any of the following notice provisions if not relevant to the limited use for which it seeks CPNI:
  - o ComNet need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;

- o ComNet need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;
- o ComNet need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as it explains to customers that the scope of the approval it seeks is limited to one-time use; and
- o ComNet may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as it clearly communicates that the customer can deny access to his or her CPNI for the call.

## **8. Training**

- a) ComNet shall train its personnel as to when they are and are not authorized to use CPNI.
- b) ComNet shall have an express disciplinary process in place.

## **9. Records**

- a) ComNet shall maintain a record of its own and its affiliates' sales and marketing campaigns that use its customers' CPNI.
- b) ComNet shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record shall include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign.
- c) ComNet shall maintain the record for a minimum of one year.

## **10. Reviews and Reporting**

- a) ComNet shall establish a supervisory review process regarding its compliance with federal CPNI rules for outbound marketing situations.
- b) ComNet shall maintain records of its compliance for a minimum period of one year.
- c) Sales personnel shall obtain supervisory approval of any proposed outbound marketing request for customer approval.
- d) ComNet shall have an officer, as an agent, sign and file with the Federal Communications Commission a compliance certificate on an annual basis. The officer shall state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's rules.

- e) ComNet shall provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the Commission's rules.
- f) ComNet shall also include an explanation of any actions taken against data brokers and a summary in the past year concerning the unauthorized release of CPNI. ComNet shall file this explanation annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.
- g) ComNet shall provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that the consumers' inability to opt-out is more than an anomaly.
  - o The notice shall be in the form of a letter, and shall include ComNet's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

#### **11. Safeguarding the Disclosure of CPNI**

- a) ComNet shall take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.
- b) ComNet shall properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.
- c) ComNet shall not disclose call detail information over the telephone, based on customer-initiated contact, unless the customer first provides ComNet with a password that is not prompted by ComNet asking for readily available biographical information, or account information.
  - o If the customer does not provide a password, ComNet shall only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record.
  - o If the customer is able to provide call detail information to ComNet during a customer-initiated call without assistance, then ComNet is permitted to discuss the call detail information provided by the customer.
- d) ComNet shall authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a ComNet's account.
  - o Once authenticated, the customer may only obtain online access to CPNI related to a ComNet's service account through a password that is not prompted by ComNet asking for readily available biographical information, or account information.

- e) ComNet may disclose CPNI to a customer who, at a ComNet's retail location, first presents to ComNet or its agent a valid photo ID matching the customer's account information.
- f) ComNet shall authenticate the customer without the use of readily available biographical information, or account information, to establish a password. ComNet may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method shall not prompt the customer for readily available biographical information, or account information.
  - o If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described above.
- g) ComNet shall notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.
  - o This notification is not required when the customer initiates service, including the selection of a password at service initiation.
  - o This notification may be through a ComNet originated voicemail or text message to the telephone number of record, or by mail to the address of record, and shall not reveal the changed information to be sent to the new account information.
- h) ComNet may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses ComNet's protection of CPNI.

## 12. Security Breaches

- a) ComNet shall notify law enforcement of a breach of its customers' CPNI.
- b) ComNet shall notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or federal rules, until it has completed the process of notifying law enforcement.
- c) As soon as practicable, and in no event later than seven business days, after reasonable determination of the breach, ComNet shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility.
- d) Notwithstanding any state law to the contrary, ComNet shall not notify customers or disclose the breach to the public until seven full business days have passed after notification to the USSS and the FBI except as provided below.

- o If ComNet believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed above, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. ComNet shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.
  - o ComNet may be directed not to disclose or notify for an initial period of up to 30 days if the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify ComNet when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to ComNet, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by ComNet.
- e) After ComNet has completed the process of notifying law enforcement, it shall notify its customers of a breach of those customers' CPNI.
- f) ComNet shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI and notifications made to customers. The record shall include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. ComNet shall retain the record for a minimum of two years.
- g) As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used or disclosed CPNI.



[Home \(https://www.comnet-telecom.us/\)](https://www.comnet-telecom.us/) > Privacy Policy

## Important Notice

By accessing this website and any of its pages the users are agreeing to the terms set out below and by continuing to use this website following the posting of any changes to these terms will signify the users' consent to the changes made. The Company may change this Privacy Policy from time to time. The Company will not reduce the users' rights under this Privacy Policy without the users' explicit consent. If changes are significant, the Company will provide a more prominent notice (including, for certain services and products, email notification of Privacy Policy changes).

The Chinese translation of this Privacy Policy is for reference only. In case of any discrepancy between the English version and the Chinese version, the English version shall prevail.

## Internet Privacy Policy Statement

In addition to the Company's duty of confidentiality to customers, the Company shall at all times observe all applicable data protection law in collecting, maintaining and using the personal data of customers.

If the users do not wish the Company to use or provide to other persons their personal data for use in direct marketing, they may exercise their opt-out right by notifying the Company.

The Company will not collect any personal data that identifies a user to this website unless specified otherwise herein. Only the pages of this website visited will be recorded. Such information will be used to prepare aggregate information about the number of visitors to the website and general statistics on usage patterns of the website. Some of this information will be gathered through the use of "cookies". For details of cookies, please refer to the Cookies Policy.

In order to provide the services and products, the Company may process certain personal data about the users. Any information relating to an identified or identifiable natural person will be regarded as "personal data", information which cannot be used to identify a natural person is "anonymous data" which is not the subject herein. The type of personal data that the Company collects depends on how the users use such services and products.

Personal data and content may be collected. The Company collects the users email address, telephone number and other information the users provide when they use the services and products, including without limitation:

- Download publications;
- Register an account for the Company's services and products;
- Participate in "join our mailing list" initiatives;
- Participate in bulletin boards, discussion or message forums;
- And Seeking technical and customer supports.

Once the users follow the Company's official account(s) in third parties' application, such as Wechat or Facebook, the Company may access the information on the users' open ID, profile photo, nickname, gender, country/region/city, the starting time of following the Company's official account(s) and status of the users' relevant account(s) from these third parties' application platform automatically for the purposes of pushing notification messages and performing statistical analysis.

Personal data about transactions made on the services and products. If the users use their accounts for purchasing certain services and products, the Company collects information about the purchase or transaction. This includes payment information, such as the users' credit or debit card number and other card information, other account and authentication information, and billing, shipping and contact details.

Intended use of the personal data. The Company uses the personal data (subject to choices the users make) for the following purposes:

- to deliver the services and products the users choose;
- to provide technical and customer support;
- to develop, test and improve the Company's services and products, including by conducting surveys and research, and testing and troubleshooting new products and features;
- to provide measurement, analytics for the Company's other services and products; and
- to investigate when the Company have a good-faith belief that it is necessary to detect, prevent and address fraud, unauthorized use of the services and products, violations of the Company's any terms or policies, or other harmful or illegal activity.

The Company will only use the personal data to send the marketing materials if the Company have the users' consent.

Users who do not allow the Company to use their information in their accounts collected through third parties' application in the above manner may at any time unfollow the Company's official account(s). In such event, users may not be able to use the services and products provided in such official account(s).

Share personal data. Subject to the applicable data protection laws, the Company may provide personal data to vendors and service providers who support the Company's business, such as by providing technical infrastructure services, providing customer service, facilitating payments or conducting surveys. The Company will use its best endeavor to ensure each of these vendors and service providers not to disclose or use the personal data for any other purposes.

The Company may share the users' personal data in response to a legal request (e.g. a search warrant, court order or subpoena) or if the Company has a good-faith belief that the law requires the Company to do so. This may include responding to legal requests from jurisdictions outside of the State of California when the Company has a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction and is consistent with internationally recognized standards.

Personal data the Company collected is a business asset. If the Company is acquired by a third party as a result of a transaction such as a merger, acquisition, or asset sale or if the Company's assets are acquired by a third party in the event the Company go out of business or enter bankruptcy, some or all of the assets, including the personal data, will be disclosed or transferred to a third party acquirer in connection with the transaction.

Transfer of personal data. Depends on the nature of the services and products, the users' personal data will likely be transferred and stored in a country outside of their home country, whose data protection laws may not be the same as in the users' home country. Such transfer is necessary for the performance of the services and products the users choose. Purchasing certain services and products will signify the users' explicitly consented to the proposed transfer.

Duration of the storages of personal data. The Company stores personal data until it is no longer necessary to provide the services and products or upon request of the users. This is a case-by-case determination that depends on things such as the nature of data, the purpose of the collection and processing and relevant legal or operational retention needs.

For services and products involving electronic communications or transactions submitted to the Company's systems for processing or transmission which may contain personal data, the Company will only process such personal data for the purpose of effectively providing the relevant services and product. Content of the electronic communications or transactions may be

stored on the Company's live systems or in the Company data archives for operational purposes such as reporting and trouble shooting. The Company will delete message content completely from the systems and data archives when it is no longer required for operational purposes.

Personal data can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation or investigations of possible violations of the Company's terms or policies, or otherwise to prevent any harm. The Company also retains information from accounts disabled for at least a year to prevent repeat abuse, other terms violations, breach or potential breach of applicable laws.

**Sensitive information:** Sensitive information includes information relating to (i) race or ethnic origin; (ii) political opinions; religious or other similar beliefs; (iii) trade union membership; and (iv) physical or mental health; sexual life or criminal records. The Company will not request the users to provide sensitive information of this nature. If the users provide sensitive information voluntarily for any reason, the users explicitly consent to the Company's use of the sensitive information in the ways described in this Privacy Policy or as described at the point where they choose to disclose this information.

**Users' Rights and Choices:** If the users are based in European Economic Area or in any country/area that mandates similar rights, the users can:

- Request access to and a copy of the personal data that the Company holds on the users;
- Delete, correct or update the personal data via altering the setting in their accounts or Contact the Company;
- Request the Company to stop using the personal data, including for marketing and promotional purposes;
- Have the personal data transferred to another organization (where it is technically feasible);
- Complain to a regulator. The Company appreciates the chance to deal with the users concerns directly so the Company prefers the users to Contact the Company first.

The law provides exceptions to these rights in certain circumstances. The Company will provide reason to the users if they have any concern. **Consent:** The Company only collects or process personal data if it is specifically and voluntarily provided by the users. If the users provide the Company with personal data about another person, they shall warrant that they have that person's consent to do so and that person has given explicit consent for the Company to collect or process their personal data for the purpose for which such users submitted it to the Company. To the fullest extent allowed by applicable laws, the users shall fully indemnify, defend and hold harmless, the Company, the Group Members, their respective officers, employees, agents, representatives, consultants, and contractors from and against any and all loss, costs, penalties, fines, damages, claims, expenses (including attorney's fees) or liabilities arising out of, resulting from, or in connection with the breach of this clause.

## Contact the Company

Request for access to personal data or correction of personal data or for information regarding policies and practices on personal data and kinds of personal data held should be addressed to: [support@comnetechs.com](mailto:support@comnetechs.com) (<mailto:support@comnetechs.com>)

**PAGES C-16 THROUGH C-20 REDACTED AS  
CONFIDENTIAL**

**EXHIBIT D**

**2018 Slide Presentation to the Department of Justice**

**REDACTED – FOR PUBLIC INSPECTION**

**ATTACHMENT REDACTED IN ITS ENTIRETY AS  
CONFIDENTIAL**



**EXHIBIT F**

**2009 Pacific Networks Corp. IT Security Policy**

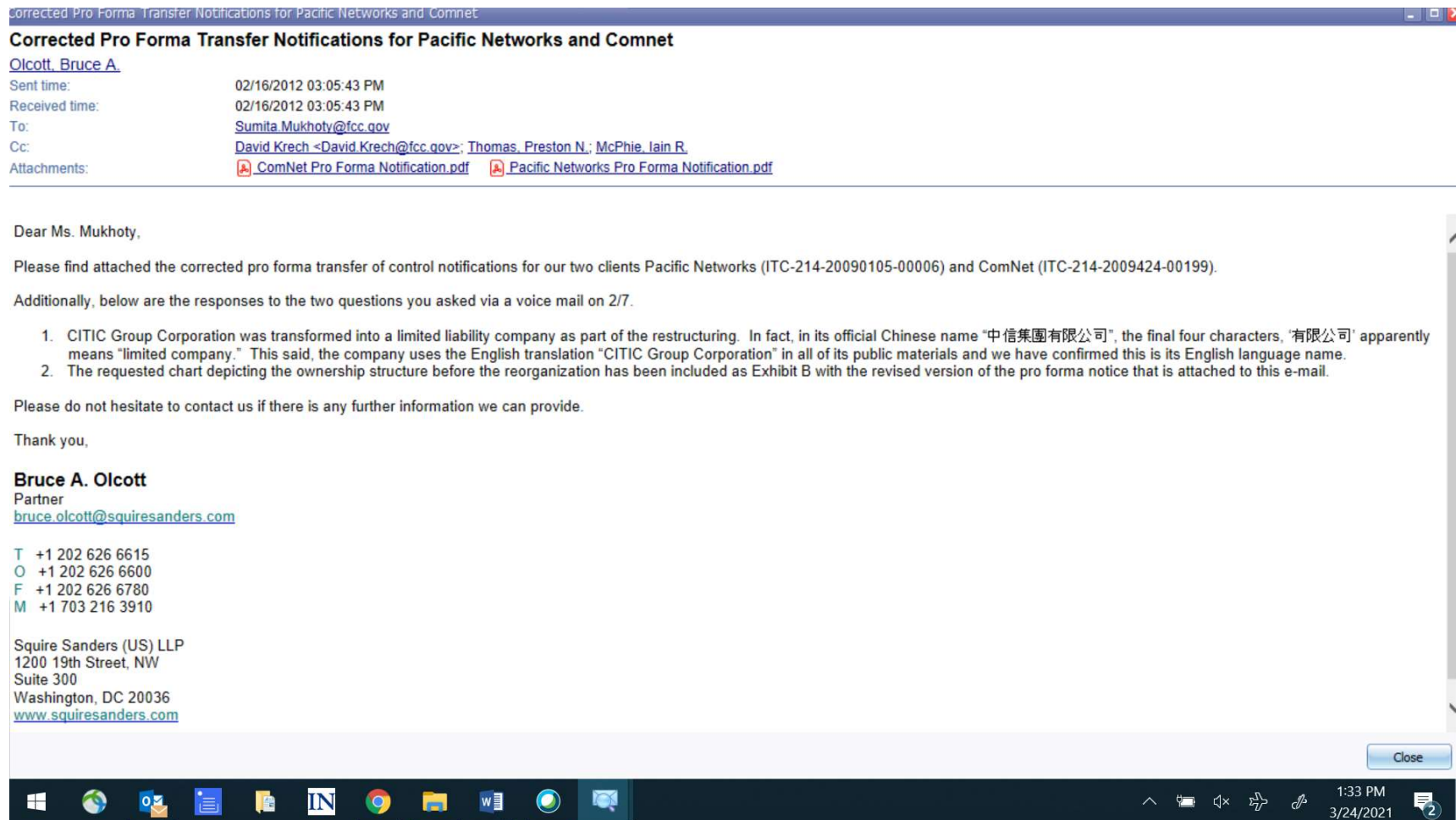


**REDACTED – FOR PUBLIC INSPECTION**

**ATTACHMENT REDACTED IN ITS ENTIRETY AS  
CONFIDENTIAL**

**EXHIBIT G**

**Cover Email and Corrected Notifications for 2012 Pro Forma Transfer**





SQUIRE SANDERS (US) LLP  
1200 19TH STREET, NW  
SUITE 300  
WASHINGTON, DC 20036

O +1 202 626 6600  
F +1 202 626 6780  
SQUIRESANDERS.COM

Bruce A. Olcott  
+1 202 626 6615  
bruce.olcott@squiresanders.com

February 16, 2012

**VIA ELECTRONIC FILING**

Marlene Dortch  
Secretary  
Federal Communications Commission  
445 12 Street, SW  
Washington, DC 20554

**Re: Pro Forma Transfer of Control of International Section 214 Authorizations  
File No. ITC-214-20090424-00199  
ComNet (USA) LLC**

Dear Ms. Dortch:

ComNet (USA) LLC ("ComNet"), pursuant to section 63.24 of the Commission's Rules, 47 C.F.R. § 63.24, hereby notifies the Commission of the *pro forma* restructuring of CITIC Group, the ultimate parent company of ComNet, effective as of December 27, 2011.

As part of a broader corporate reorganization to facilitate financial, business, and administrative objectives, CITIC Group Corporation (formerly known as CITIC Group<sup>1</sup>) has taken the several restructuring actions detailed below.

**The CITIC Group Restructuring**

CITIC Group, the ultimate controlling shareholder of 214 grantee ComNet, has completed a restructuring involving the following:

---

<sup>1</sup> CITIC Group's name change accompanied a change in corporate form, as explained below in item (1).

February 16, 2012

Page 2

- (1) The transformation of CITIC Group from a state-owned enterprise into CITIC Group Corporation, a state-owned limited liability company, which involved a change of the company's industrial and commercial registration;
- (2) The establishment, along with CITIC Group Corporation's wholly owned subsidiary Beijing CITIC Enterprise Management Co., Ltd., of a new joint stock company, CITIC Limited, to hold a substantial portion of the existing business and assets of CITIC Group Corporation, including CITIC Group Corporation's existing indirect 60.59% interest in CITIC Telecom International Holdings Limited (formerly CITIC 1616 Holdings Limited), which indirectly holds 100% interest in ComNet; and
- (3) The addition of CITIC Investment (HK) Limited as a wholly owned subsidiary of CITIC Limited as an indirect holder of an approximately 37% interest in CITIC Pacific Limited, an indirect holder of the group's 60.59% interest in CITIC Telecom International Holdings Limited.

Pursuant to 63.24(f), the attached Exhibit A provides responses to 63.18(b), (d), and (h) in connection with the restructuring described above. A pair of charts illustrating the ownership structure before and after the reorganization are attached as Exhibit B.<sup>2</sup>

ComNet certifies that this assignment is *pro forma* as defined in paragraph (a)(5) of section 63.24 of the Commission's Rules and, together with all previous *pro forma* transactions, does not result in a change of the carrier's ultimate control.

Answer to question 10: ComNet, originally authorized as CM Tel (USA) LLC before a name change,<sup>3</sup> is authorized under Section 214 to provide facilities-based and resale service between the United States and all permissible foreign points except China and Hong Kong.<sup>4</sup> The principal business address, telephone number, and point of contact for ComNet is as follows:

ComNet (USA) LLC  
 700 S. Flower Street  
 Suite 750  
 Los Angeles, CA 90017  
 Attn: Linda Peng  
 (213) 488-1951 – Telephone  
 (213) 488-1491 – Facsimile  
 lindapeng@comnet-telecom.com

<sup>2</sup> The charts attached as Exhibit B are updated and simplified versions of the diagram provided with the original applications. The charts show only those entities in the direct line of control between CITIC Group Corporation and grantee ComNet. They omit non-CITIC affiliated organizations that do not possess controlling interests.

<sup>3</sup> File No. ITC-214-20090424-00199, *See* Public Notice DA No. 10-499.

<sup>4</sup> File No. ITC-214-20090424-00199

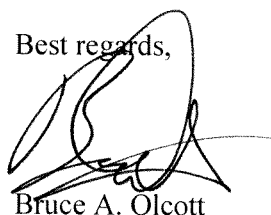
February 16, 2012  
Page 3

Correspondence or communications regarding this notice should be directed to:

Bruce Olcott  
Squire Sanders (US) LLP  
1200 19th Street, NW  
Suite 300  
Washington, DC 20036  
(202) 626-6615 – Telephone  
(202) 626-6780 – Facsimile  
Bruce.Olcott@squiresanders.com – Email

Upon request ComNet is prepared to answer any questions, or present additional information about the reorganization. If you have any questions or require additional information, please call me at (202) 626-6615.

Best regards,

A handwritten signature in black ink, appearing to read 'Bruce A. Olcott', with a large, stylized initial 'B'.

Bruce A. Olcott

36 OFFICES IN 17 COUNTRIES

SQUIRE SANDERS (US) LLP IS PART OF THE INTERNATIONAL LEGAL PRACTICE SQUIRE SANDERS WHICH OPERATES WORLDWIDE THROUGH A NUMBER OF SEPARATE LEGAL ENTITIES.

PLEASE VISIT [SQUIRESANDERS.COM](http://SQUIRESANDERS.COM) FOR MORE INFORMATION.

ComNet (USA) LLC  
*Pro Forma* Transfer of Control Notice  
File No. ITC-214-20090424-00199

**Exhibit A**

**§ 63.18 Equity Owner Information**

ComNet (USA) LLC  
*Pro Forma* Transfer of Control Notice  
 File No. ITC-214-20090424-00199

**Pacific Networks Corp.**

Address: c/o 700 S. Flower Street  
 Suite 750  
 Los Angeles, CA 90017  
 Principal Business: International resold voice and data  
 Place of Incorporation: Delaware  
 Shareholding in Applicant: Directly owns and controls 100% of ComNet.

**Pacific Choice International Limited**

Address: c/o 25/F., CITIC Telecom Tower  
 93 Kwai Fuk Road  
 Kwai Chung, New Territories  
 Hong Kong  
 Principal Business: Investment holding company for systems integration business  
 focused in serving telecommunications operators  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Pacific Networks Corp.

**CITIC Telecom International Holdings Limited**

Address: 25/F., CITIC Telecom Tower  
 93 Kwai Fuk Road  
 Kwai Chung, New Territories  
 Hong Kong  
 Principal Business: Holding company and performs sales and marketing functions  
 primarily for affiliated companies  
 Place of Incorporation: Hong Kong  
 Shareholding in Applicant: Directly owns and controls 100% of Pacific Choice International  
 Limited (resulting in 100% indirect ownership and control of the  
 Applicant).

**Silver Log Holdings Ltd.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns approximately 17.01% of CITIC Telecom International  
 Holdings Limited (resulting in approximately 17.01% indirect ownership of  
 the Applicant).

**Onway Assets Holdings Ltd.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong



ComNet (USA) LLC  
*Pro Forma* Transfer of Control Notice  
 File No. ITC-214-20090424-00199

Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Silver Log Holdings Ltd. (resulting in approximately 17.01% indirect ownership of the Applicant).

**Ease Action Investments Corp.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns approximately 39.47% of CITIC Telecom International Holdings Limited (resulting in approximately 39.47% indirect ownership of the Applicant).

**Ferretti Holdings Corp.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Ease Action Investments Corp. (resulting in approximately 39.47% indirect ownership of the Applicant).

**Richtone Enterprises Inc.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns approximately 4.11% of CITIC Telecom International Holdings Limited (resulting in approximately 4.11% indirect ownership of the Applicant).

**Peganin Corp.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Richtone Enterprises Inc. (resulting in approximately 4.11% indirect ownership of the Applicant).

ComNet (USA) LLC  
Pro Forma Transfer of Control Notice  
File No. ITC-214-20090424-00199

**Douro Holdings Inc.**

Address: c/o 32/F, CITIC Tower  
1 Tim Mei Avenue, Central  
Hong Kong

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns and controls 100% of each of Onway Assets Holdings Ltd., Ferretti Holdings Corp. and Peganin Corp., and thus indirectly owns approximately 60.59% of CITIC Telecom International Holdings Limited (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Pacific Communications Limited**

Address: 32/F, CITIC Tower  
1 Tim Mei Avenue, Central  
Hong Kong

Principal Business: Investment holding company

Place of Incorporation: Bermuda

Shareholding in Applicant: Directly owns and controls 100% of Douro Holdings Inc. (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Effectual Holdings Corp.**

Address: c/o 32/F, CITIC Tower  
1 Tim Mei Avenue, Central  
Hong Kong

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns and controls 100% of CITIC Pacific Communications Limited (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Crown Base International Limited**

Address: c/o 32/F, CITIC Tower  
1 Tim Mei Avenue, Central  
Hong Kong

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns and controls 100% of Effectual Holdings Corp. (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

ComNet (USA) LLC  
*Pro Forma* Transfer of Control Notice  
 File No. ITC-214-20090424-00199

**CITIC Pacific Limited**

Address: 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong

Principal Business: Hong Kong-based conglomerate company, its major businesses are special steel manufacturing, iron ore mining and property development in mainland China. Other businesses include energy and civil infrastructure. It also holds controlling interests in Dah Chong Hong Holdings Limited and CITIC Telecom International Holdings Limited.

Place of Incorporation: Hong Kong

Shareholding in Applicant: Directly owns and controls 100% of Crown Base International Limited (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Full Chance Investments Limited**

Address: c/o 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns approximately 12.342% of CITIC Pacific Limited (resulting in approximately 12.342% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Newease Investments Limited**

Address: c/o 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns approximately 12.342% of CITIC Pacific Limited (resulting in approximately 12.342% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Skyprofit Holdings Limited**

Address: c/o 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns approximately 12.342% of CITIC Pacific Limited (resulting in approximately 12.342% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

ComNet (USA) LLC  
*Pro Forma* Transfer of Control Notice  
 File No. ITC-214-20090424-00199

**CITIC Hong Kong (Holdings) Limited**

Address: c/o Capital Mansion  
 6 Xinyuan South Road  
 Chaoyang District, Beijing 100004  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Indirectly owns approximately 20.482% of CITIC Pacific Limited (resulting in approximately 20.482% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Investment (HK) Limited**

Address: Room 2118, Hutchison House  
 10 Harcourt Road  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: Hong Kong  
 Shareholding in Applicant: Directly owns 100% of each of Full Chance Investments Limited, Newease Investments Limited and Skyprofit Holdings Limited, and thus indirectly owns approximately 37.026% of CITIC Pacific Limited (resulting in approximately 37.026% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Limited**

Address: 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004  
 Principal Business: Investment holding company  
 Place of Incorporation: People's Republic of China  
 Shareholding in Applicant: Directly owns 100% of both CITIC Investment (HK) Limited and CITIC Hong Kong (Holdings) Limited, and thus indirectly owns approximately 57.508% of CITIC Pacific Limited (resulting in 100% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Beijing CITIC Enterprise Management Co., Ltd.**

Address: c/o 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004  
 Principal Business: Investment holding company  
 Place of Incorporation: People's Republic of China  
 Shareholding in Applicant: Directly owns 0.1% of CITIC Limited, and thus indirectly owns approximately 5.7508% of CITIC Pacific Limited (resulting in

ComNet (USA) LLC  
*Pro Forma* Transfer of Control Notice  
 File No. ITC-214-20090424-00199

approximately 5.7508% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Group Corporation**

Address: 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004  
 Principal Business: Investment holding company  
 Place of Incorporation: People's Republic of China  
 Shareholding in Applicant: Directly owns 100% of Beijing CITIC Enterprise Management Co., Ltd, and directly owns 99.9% of CITIC Limited, (resulting in 100% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

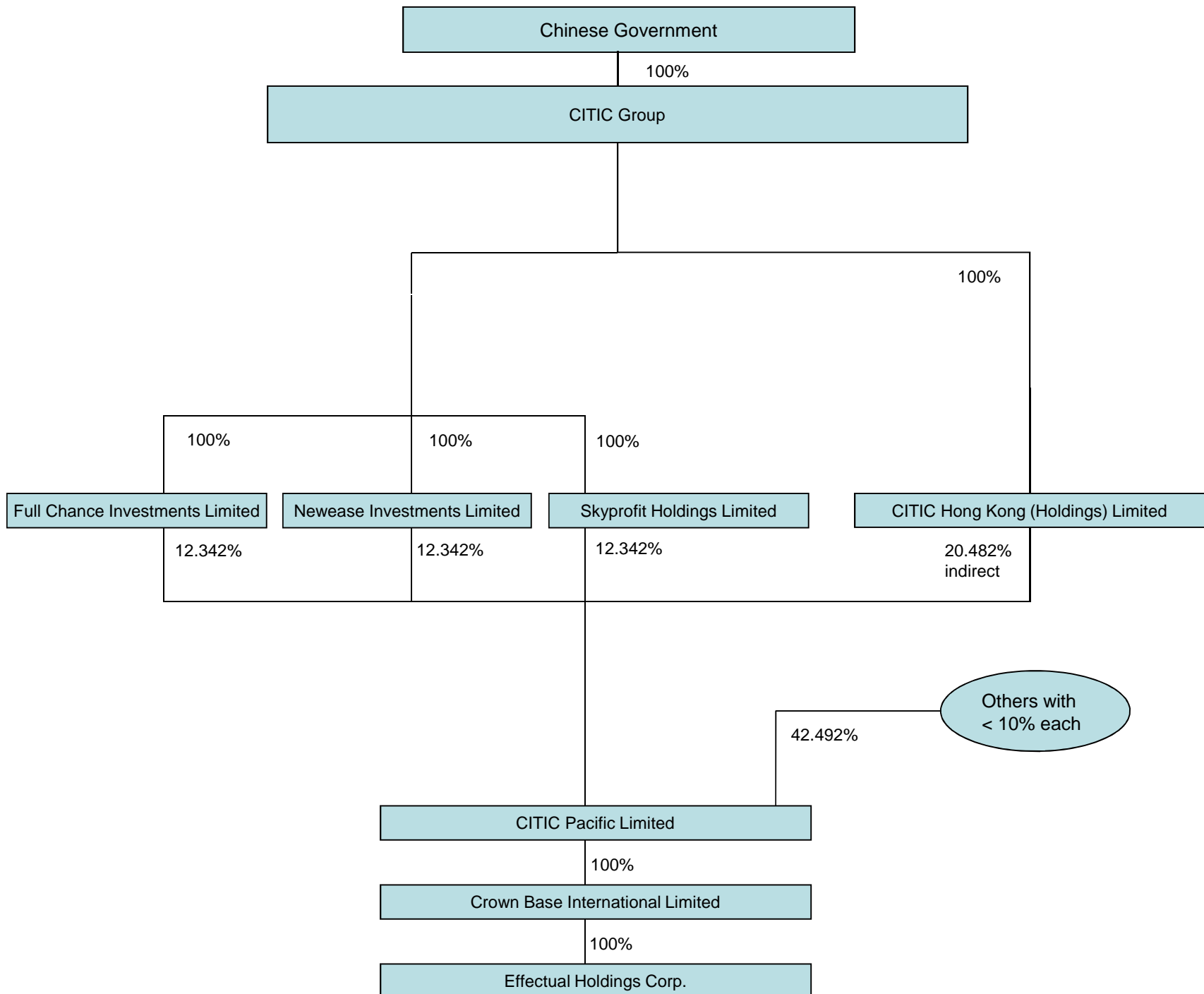
**Assets Supervision and Administration Commission of the State Council of China**

Address: Government of China  
 Beijing, China  
 Place of Incorporation: China  
 Principal Business: Government  
 Shareholding in Applicant: Owns 100% of CITIC Group Corporation (resulting in 100% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

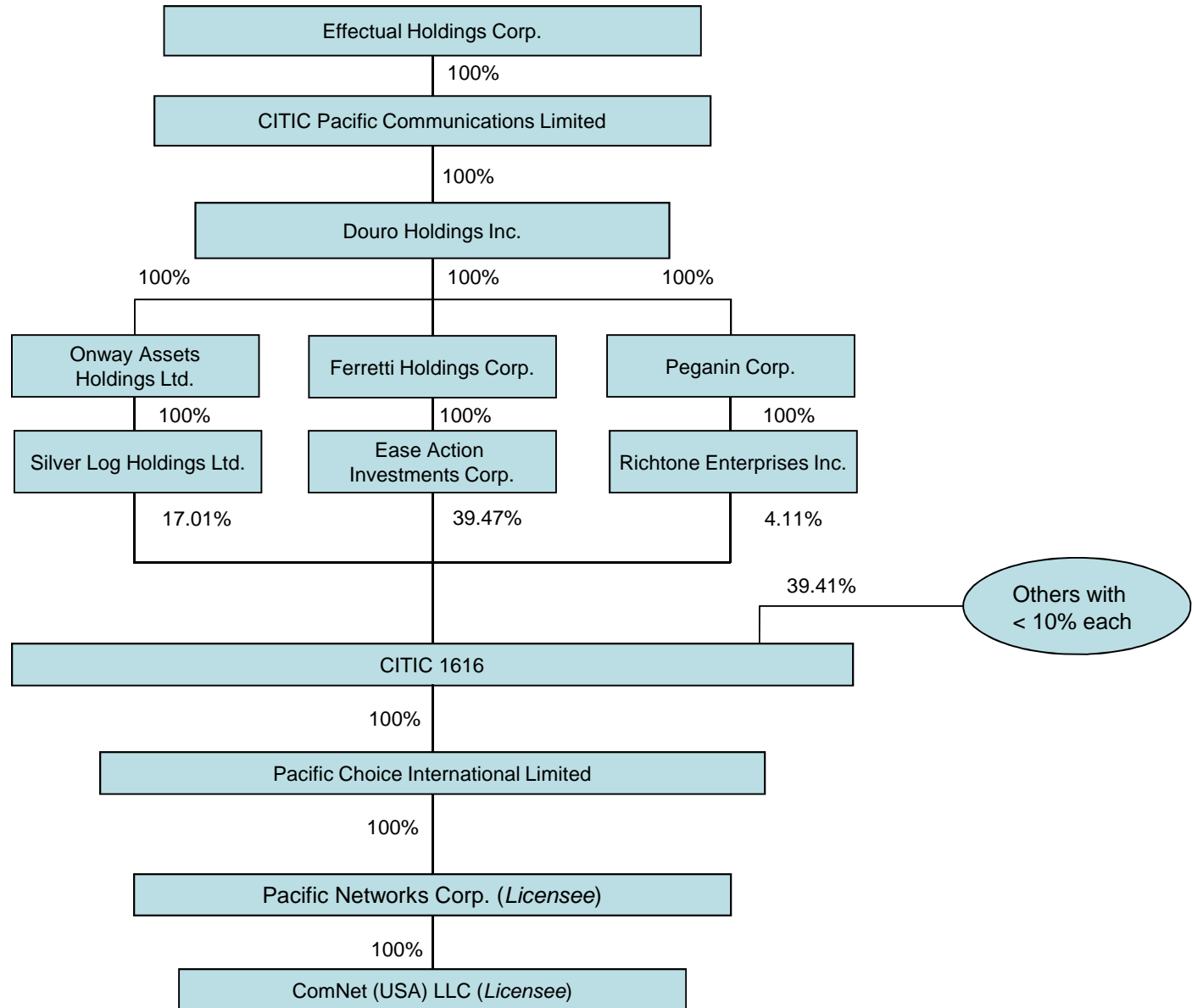
**Exhibit B**

**Corporate Structure Charts Pre-  
and Post-Reorganization**

**Pacific Networks Corp. and ComNet (USA) LLC  
Pre-Reorganization Ownership Structure**

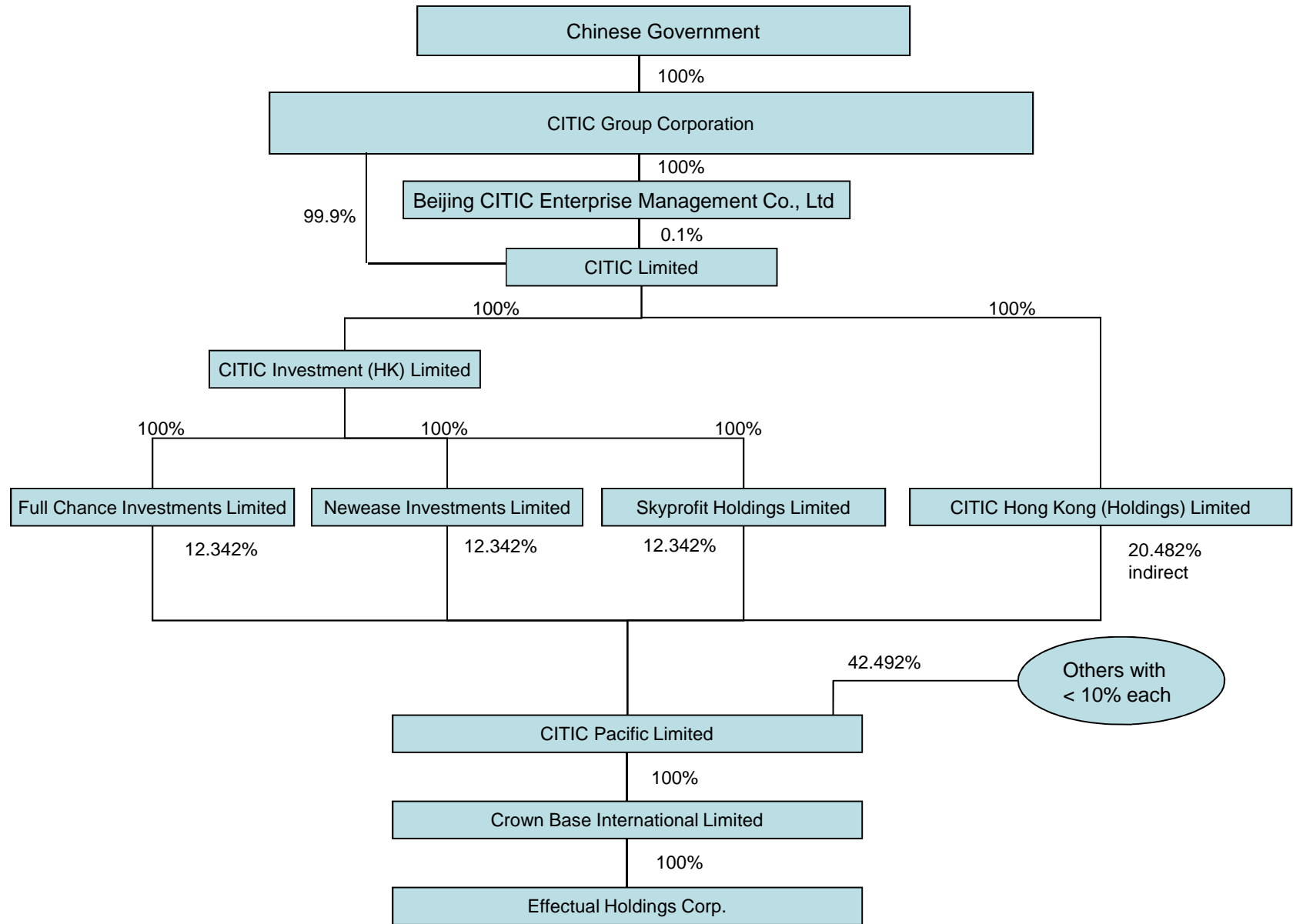


**Pacific Networks Corp. and ComNet (USA) LLC  
 Pre-Reorganization Ownership Structure**

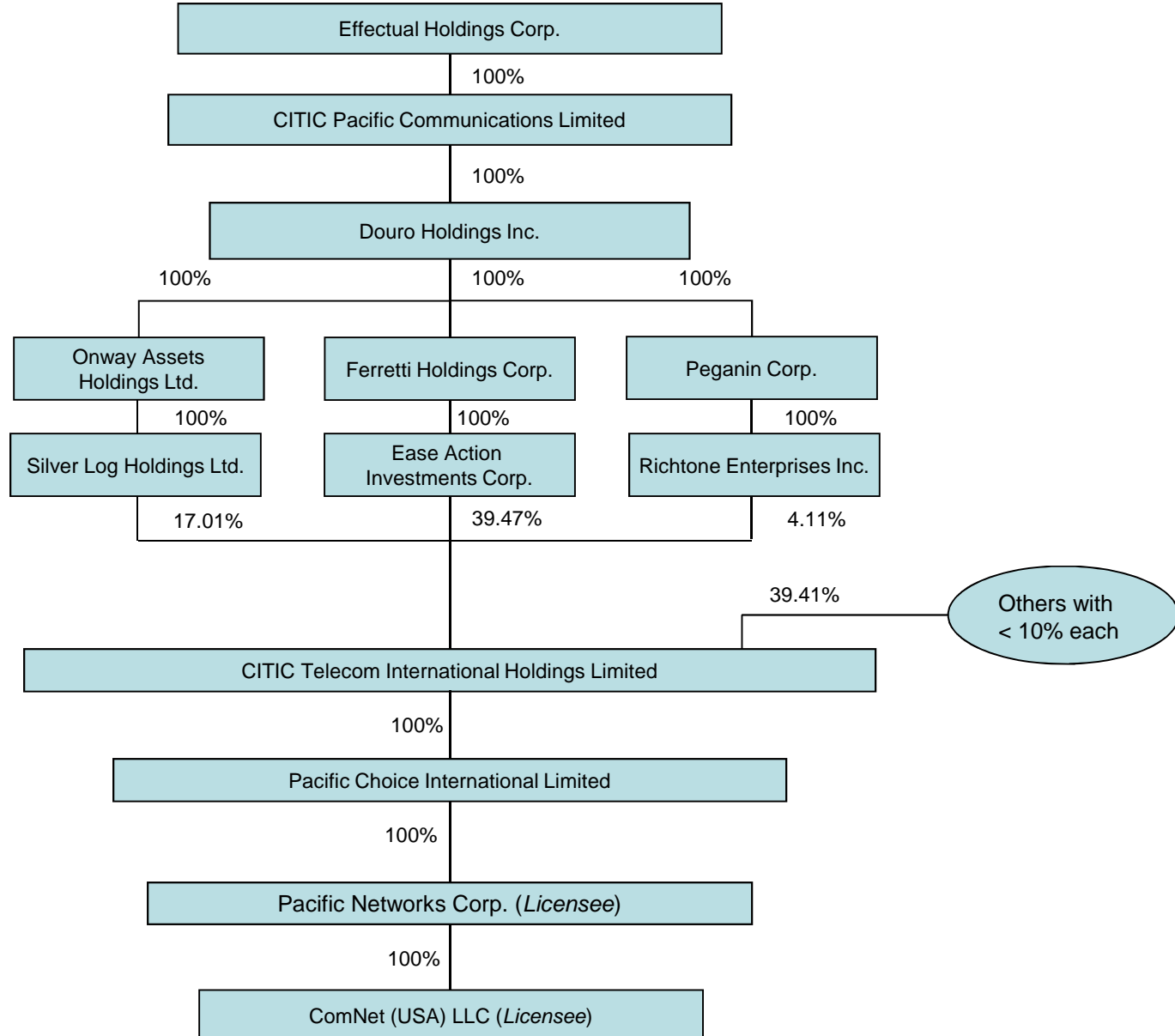




**Pacific Networks Corp. and ComNet (USA) LLC  
 Post-Reorganization Ownership Structure**



**Pacific Networks Corp. and ComNet (USA)  
 LLC  
 Post-Reorganization Ownership Structure**





SQUIRE SANDERS (US) LLP  
1200 19TH STREET, NW  
SUITE 300  
WASHINGTON, DC 20036

O +1 202 626 6600  
F +1 202 626 6780  
SQUIRESANDERS.COM

Bruce A. Olcott  
+1 202 626 6615  
bruce.olcott@squiresanders.com

February 16, 2012

**VIA ELECTRONIC FILING**

Marlene Dortch  
Secretary  
Federal Communications Commission  
445 12 Street, SW  
Washington, DC 20554

**Re: Pro Forma Transfer of Control of International Section 214 Authorizations  
File No. ITC-214-20090105-00006  
Pacific Networks Corp.**

Dear Ms. Dortch:

Pacific Networks Corp. ("Pacific Networks"), pursuant to section 63.24 of the Commission's Rules, 47 C.F.R. § 63.24, hereby notifies the Commission of the *pro forma* restructuring of CITIC Group, the ultimate parent company of Pacific Networks, effective as of December 27, 2011.

As part of a broader corporate reorganization to facilitate financial, business, and administrative objectives, CITIC Group Corporation (formerly known as CITIC Group<sup>1</sup>) has taken the several restructuring actions detailed below.

**The CITIC Group Restructuring**

CITIC Group, the ultimate controlling shareholder of 214 grantee Pacific Networks, has completed a restructuring involving the following:

---

<sup>1</sup> CITIC Group's name change accompanied a change in corporate form, as explained below in item (2).

February 16, 2012

Page 2

- (1) The transformation of CITIC Group from a state-owned enterprise into CITIC Group Corporation, a state-owned limited liability company, which involved a change of the company's industrial and commercial registration;
- (2) The establishment, along with CITIC Group Corporation's wholly owned subsidiary Beijing CITIC Enterprise Management Co., Ltd., of a new joint stock company, CITIC Limited, to hold a substantial portion of the existing business and assets of CITIC Group Corporation, including CITIC Group Corporations existing indirect 60.59% interest in CITIC Telecom International Holdings Limited (formerly CITIC 1616 Holdings Limited), which indirectly holds 100% interests in Pacific Networks; and
- (3) The addition of CITIC Investment (HK) Limited as a wholly owned subsidiary of CITIC Limited as an indirect holder of an approximately 37% interest in CITIC Pacific Limited, an indirect holder of the group's 60.59% interest in CITIC Telecom International Holdings Limited.

Pursuant to 63.24(f), the attached Exhibit A provides responses to 63.18(b), (d), and (h) in connection with the restructuring described above. A pair of charts illustrating the ownership structure before and after the reorganization are attached as Exhibit B.<sup>2</sup>

Pacific Networks certifies that this assignment is *pro forma* as defined in paragraph (a)(5) of section 63.24 of the Commission's Rules and, together with all previous *pro forma* transactions, does not result in a change of the carrier's ultimate control.

Answer to question 10: Grantee Pacific Networks is authorized under Section 214 to provide resale service on all United States international routes, except China and Hong Kong.<sup>3</sup> The principal business address, telephone number, and point of contact for Pacific Networks is as follows:

Pacific Networks Corp.  
 700 S. Flower Street  
 Suite 750  
 Los Angeles, CA 90017  
 Attn: Bruce A. Olcott  
 (202) 626-6615 – Telephone  
 (202) 626-6780 – Facsimile  
 Bruce.Olcott@squiresanders.com

<sup>2</sup> The charts attached as Exhibit B is an updated and simplified version of the diagram provided with the original applications. Exhibit B shows only those entities in the direct line of control between CITIC Group and grantee Pacific Networks. It omits non-CITIC affiliated organizations that do not possess controlling interests.

<sup>3</sup> File No. ITC-214-20090105-00006.


February 16, 2012  
Page 3

Correspondence or communications regarding this notice should be directed to:

Bruce Olcott  
Squire Sanders (US) LLP  
1200 19th Street, NW  
Suite 300  
Washington, DC 20036  
(202) 626-6615 – Telephone  
(202) 626-6780 – Facsimile  
Bruce.Olcott@squiresanders.com – Email

Upon request, Pacific Networks is prepared to answer any questions, or present additional information about the reorganization. If you have any questions or require additional information, please call me at (202) 626-6615.

Best regards,



Bruce A. Olcott

36 OFFICES IN 17 COUNTRIES

SQUIRE SANDERS (US) LLP IS PART OF THE INTERNATIONAL LEGAL PRACTICE SQUIRE SANDERS WHICH OPERATES WORLDWIDE THROUGH A NUMBER OF SEPARATE LEGAL ENTITIES.

PLEASE VISIT [SQUIRESANDERS.COM](http://SQUIRESANDERS.COM) FOR MORE INFORMATION.

Pacific Networks Corp.  
*Pro Forma* Transfer of Control Notice  
File Nos. ITC-214-20090105-00006

**Exhibit A**

**§ 63.18 Equity Owner Information**

Pacific Networks Corp.  
*Pro Forma* Transfer of Control Notice  
 File Nos. ITC-214-20090105-00006

**Pacific Choice International Limited**

Address: 25/F., CITIC Telecom Tower  
 93 Kwai Fuk Road  
 Kwai City, New Territories  
 Hong Kong  
 Principal Business: Investment holding company for systems integration business  
 focused in serving telecommunications operators  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Pacific Networks Corp.

**CITIC Telecom International Holdings Limited**

Address: 25/F., CITIC Telecom Tower  
 93 Kwai Fuk Road  
 Kwai City, New Territories  
 Hong Kong  
 Principal Business: Holding company and performs sales and marketing functions  
 primarily for affiliated companies  
 Place of Incorporation: Hong Kong  
 Shareholding in Applicant: Directly owns and controls 100% of Pacific Choice International  
 Limited (resulting in 100% indirect ownership and control of  
 Applicant).

**Silver Log Holdings Ltd.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns approximately 17.01% of CITIC Telecom International  
 Holdings Limited (resulting in approximately 17.01% indirect ownership of  
 the Applicant).

**Onway Assets Holdings Ltd.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Silver Log Holdings Ltd. (resulting in  
 17.01% indirect ownership of the Applicant).

**Ease Action Investments Corp.**

Address: c/o 32/F, CITIC Tower

Pacific Networks Corp.  
*Pro Forma* Transfer of Control Notice  
 File Nos. ITC-214-20090105-00006

Principal Business: 1 Tim Mei Avenue, Central  
 Hong Kong  
 Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns approximately 39.47% of CITIC Telecom International Holdings Limited (resulting in approximately 39.47% indirect ownership of the Applicants).

**Ferretti Holdings Corp.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Ease Action Investments Corp. (resulting in 39.47% indirect ownership of the Applicant).

**Richtone Enterprises Inc.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns approximately 4.11% of CITIC Telecom International Holdings Limited (resulting in 4.11% indirect ownership of the Applicant).

**Peganin Corp.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Richtone Enterprises Inc. (resulting in 4.11% indirect ownership of the Applicants).

**Douro Holdings Inc.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of each of Onway Assets Holdings Ltd., Ferretti Holdings Corp. and Peganin Corp., and thus indirectly owns



Pacific Networks Corp.  
*Pro Forma* Transfer of Control Notice  
 File Nos. ITC-214-20090105-00006

60.59% of CITIC Telecom International Holdings Limited (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Pacific Communications Limited**

Address: 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: Bermuda  
 Shareholding in Applicant: Directly owns and controls 100% of Douro Holdings Inc. (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Effectual Holdings Corp.**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of CITIC Pacific Communications Limited (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Crown Base International Limited**

Address: c/o 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: British Virgin Islands  
 Shareholding in Applicant: Directly owns and controls 100% of Effectual Holdings Corp. (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Pacific Limited**

Address: 32/F, CITIC Tower  
 1 Tim Mei Avenue, Central  
 Hong Kong  
 Principal Business: Hong Kong-based conglomerate company, its major business of which are special steel manufacturing and iron ore mining, and property development in mainland China. Other businesses include energy and civil

Pacific Networks Corp.  
*Pro Forma* Transfer of Control Notice  
 File Nos. ITC-214-20090105-00006

infrastructure. It also holds controlling interests in Dah Chong Hong Holidays Limited and CITIC Telecom International Holdings Limited.

Place of Incorporation: Hong Kong

Shareholding in Applicant: Directly owns and controls 100% of Crown Base International Limited (resulting in 100% attributable interest in and control of Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Full Chance Investments Limited**

Address: c/o 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns approximately 12.342% of CITIC Pacific Limited (resulting in approximately 12.342% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Newease Investments Limited**

Address: c/o 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns approximately 12.342% of CITIC Pacific Limited (resulting in approximately 12.342% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Skyprofit Holdings Limited**

Address: c/o 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Shareholding in Applicant: Directly owns approximately 12.342% of CITIC Pacific Limited (resulting in approximately 12.342% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Hong Kong (Holdings) Limited**

Address: c/o Capital Mansion  
 6 Xinyuan South Road  
 Chaoyang District, Beijing 100004

Principal Business: Investment holding company

Place of Incorporation: British Virgin Islands

Pacific Networks Corp.  
*Pro Forma* Transfer of Control Notice  
 File Nos. ITC-214-20090105-00006

Shareholding in Applicant: Indirectly owns approximately 20.482% of CITIC Pacific Limited (resulting in approximately 20.482% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Investment (HK) Limited**

Address: Room 2118 Hutchison House  
 10 Harcourt Road  
 Hong Kong  
 Principal Business: Investment holding company  
 Place of Incorporation: Hong Kong  
 Shareholding in Applicant: Directly owns 100% of each of Full Chance Investments Limited, Newease Investments Limited and Skyprofit Holdings Limited, and thus indirectly owns approximately 37.026% of CITIC Pacific Limited (resulting in approximately 37.026% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Limited**

Address: 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004  
 Principal Business: Investment holding company  
 Place of Incorporation: People's Republic of China  
 Shareholding in Applicant: Directly owns 100% of both CITIC Investment (HK) Limited and CITIC Hong Kong (Holdings) Limited, and thus indirectly owns approximately 57.508% of CITIC Pacific Limited (resulting in 100% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**Beijing CITIC Enterprise Management Co., Ltd.**

Address: Capital Mansion  
 6 Xinyuan South Road  
 Chaoyang District, Beijing 100004  
 Principal Business: Investment holding company  
 Place of Incorporation: People's Republic of China  
 Shareholding in Applicant: Directly owns 0.1% of CITIC Limited, and thus indirectly owns approximately 5.7508% of CITIC Pacific Limited (resulting in 5.7508% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

**CITIC Group Corporation**

Address: 6 Xinyuan Nanlu  
 Chaoyang District, Beijing 100004  
 Principal Business: Investment holding company

Pacific Networks Corp.  
*Pro Forma* Transfer of Control Notice  
 File Nos. ITC-214-20090105-00006

Place of Incorporation: People's Republic of China  
 Shareholding in Applicant: Directly owns 100% of Beijing CITIC Enterprise Management Co., Ltd, and directly owns 99.9% of CITIC Limited, (resulting in 100% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

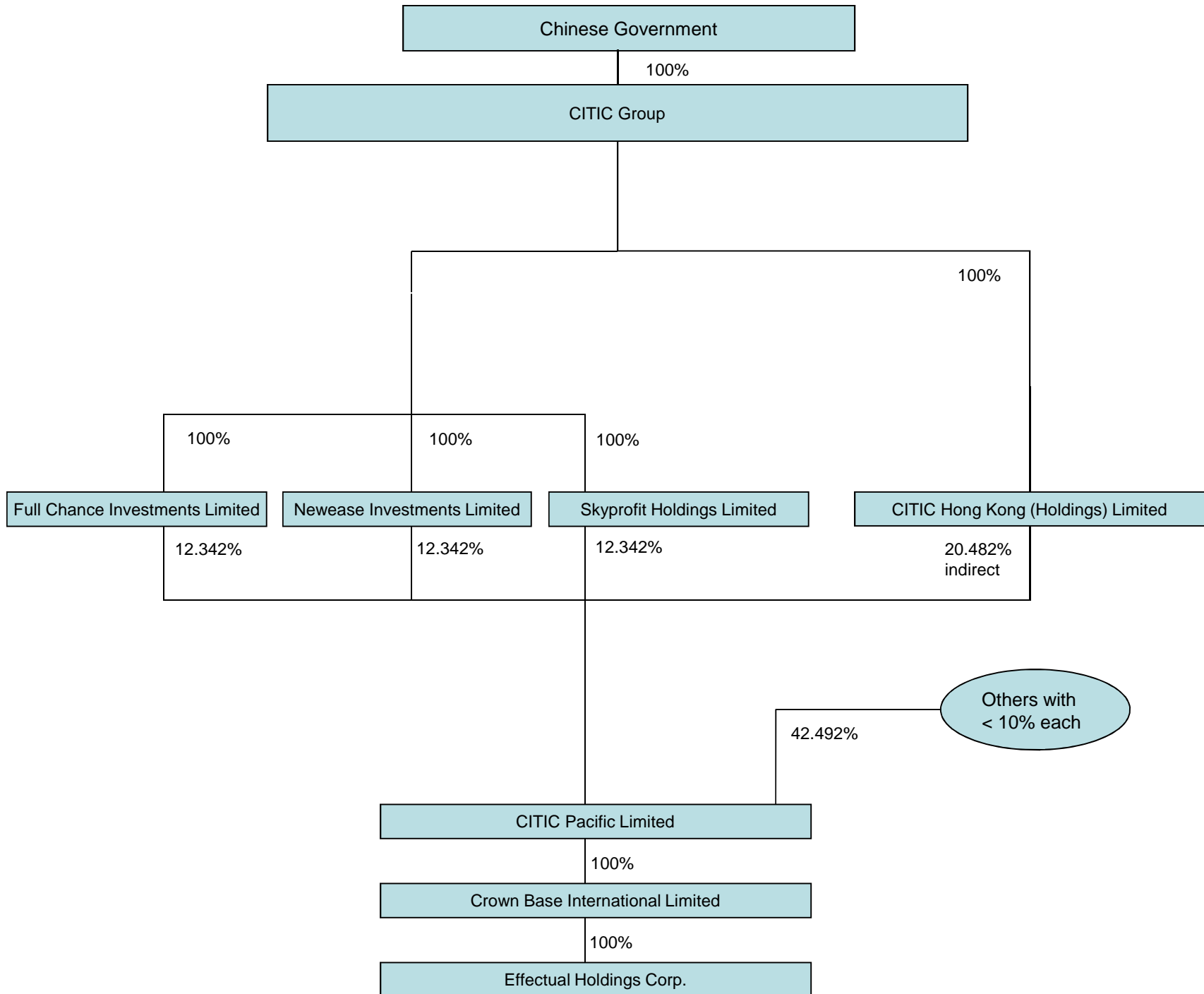
**Assets Supervision and Administration Commission of the State Council of China**

Address: Government of China  
 Beijing, China  
 Place of Incorporation: China  
 Principal Business: Government  
 Shareholding in Applicant: Directly owns 100% of CITIC Group Corporation (resulting in 100% attributable interest in the Applicant pursuant to the note to Section 63.18(h)). *See* 47 C.F.R. § 63.18(h).

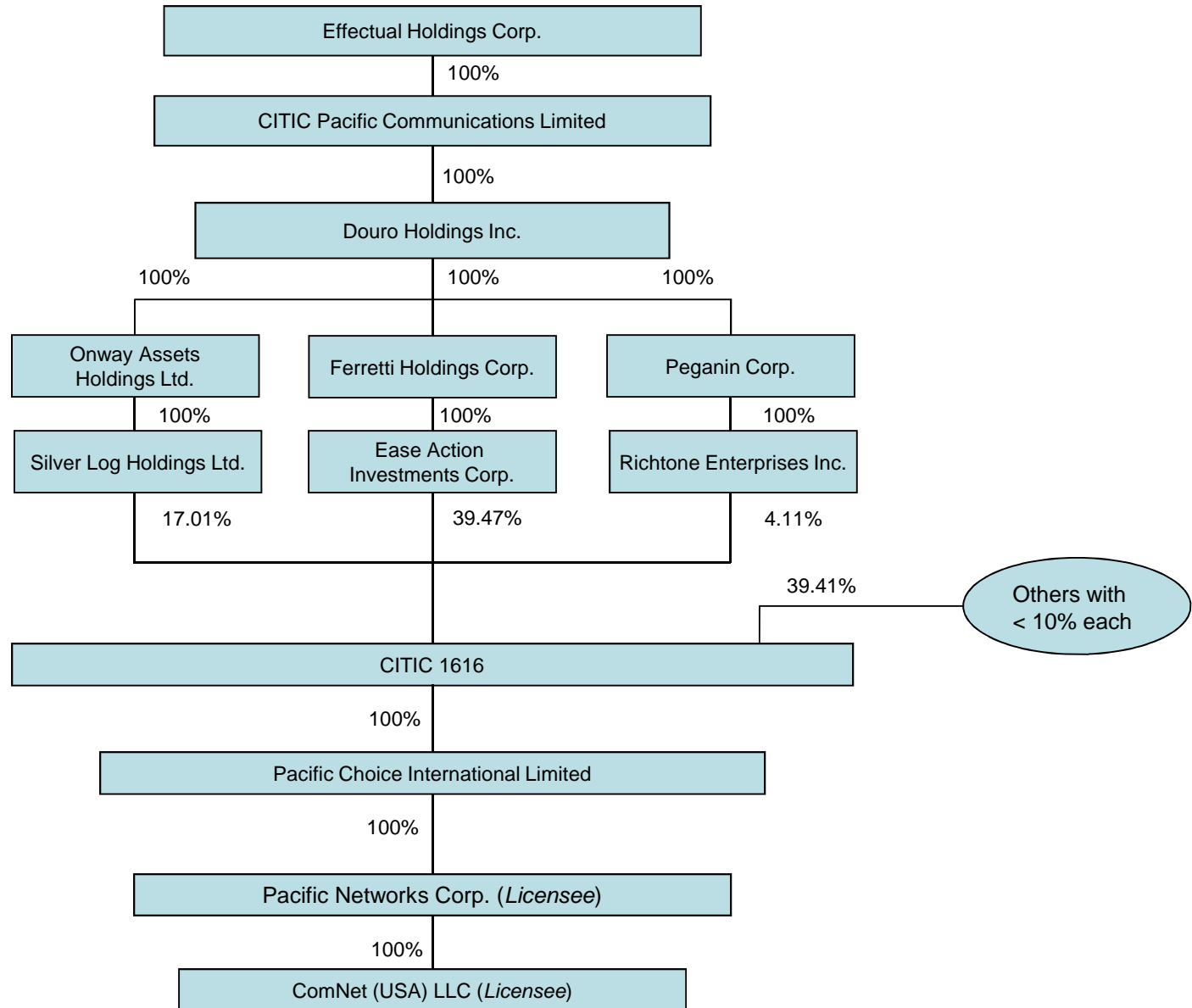
**Exhibit B**

**Corporate Structure Charts Pre-  
and Post-Reorganization**

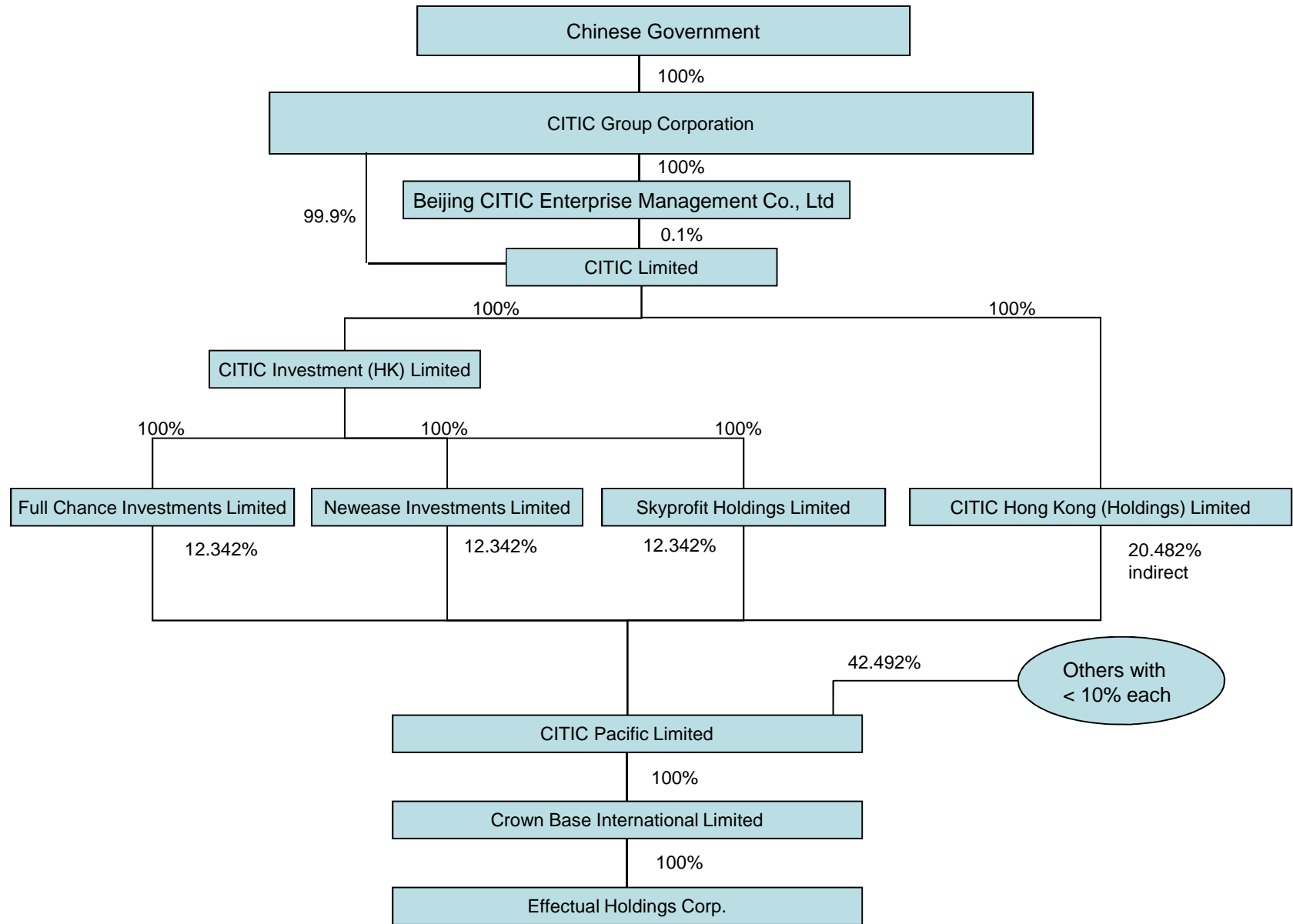
**Pacific Networks Corp. and ComNet (USA) LLC  
Pre-Reorganization Ownership Structure**



**Pacific Networks Corp. and ComNet (USA) LLC  
 Pre-Reorganization Ownership Structure**

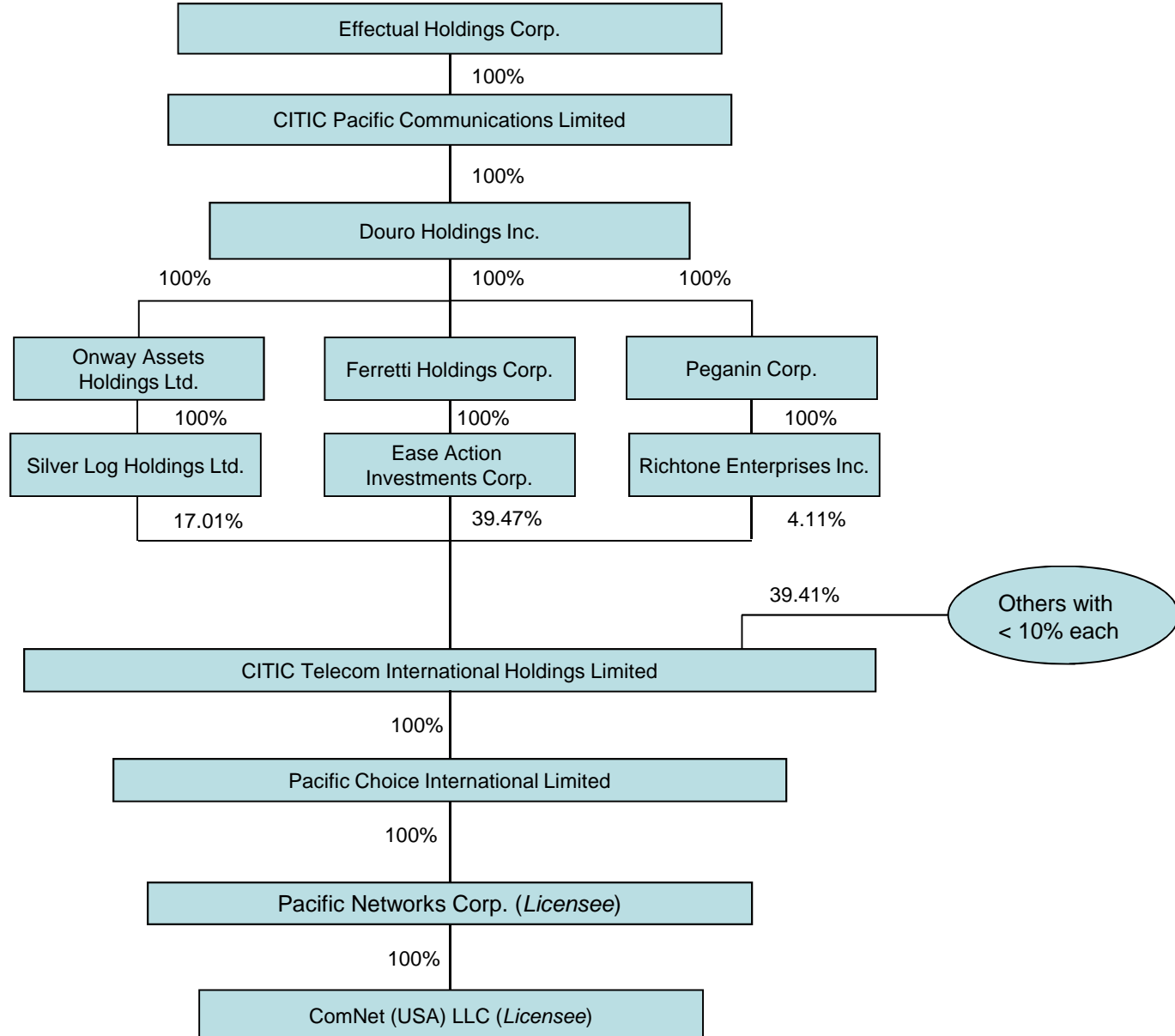


**Pacific Networks Corp. and ComNet (USA) LLC  
 Post-Reorganization Ownership Structure**





**Pacific Networks Corp. and ComNet (USA)  
 LLC  
 Post-Reorganization Ownership Structure**




**Exhibit H**

**Revised Customer Lists**

This list replaces the customer list for ComNet’s Wholesale IDD service provided at Exhibit E, page E-2 of the OSC Response.

**Wholesale IDD Service**

<b>Customer Name</b>	<b>Location (Billing)</b>
----------------------	---------------------------

This list replaces the customer list for ComNet’s VoIP service provided at Exhibit E, page E-3 of the OSC Response.

VoIP Service

Customer Name	Customer Type
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

This list replaces the customer list for ComNet’s Website/WeChat Service provided at Exhibit E, page E-3 of the OSC Response.

Website Service

Service Type	Customer Name	Customer Type	Location
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

**Exhibit I**

**Diagram for ComNet VoIP Service**

**REDACTED – FOR PUBLIC INSPECTION**

**ATTACHMENT REDACTED IN ITS ENTIRETY AS  
CONFIDENTIAL**

**Exhibit J**

**Services Agreement**

**REDACTED – FOR PUBLIC INSPECTION**

**ATTACHMENT REDACTED IN ITS ENTIRETY AS  
CONFIDENTIAL**